university of groningen / faculty of science and engineering / mathematics and applied mathematics

Mordell's Theorem Over Rational Function Fields Via Descent by 3-Isogeny

Bachelor's Project Mathematics

July 2020

Student: S.E. Bootsma

First supervisor: Dr. J.S. Müller

Second assessor: Prof. J. Top

Abstract

Mordell's theorem states that the group of rational points on an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group. This thesis considers Mordell's theorem over rational function fields of the form $\mathbb{F}_q(t)$, where q is a prime power. Assuming the existence of an $\mathbb{F}_q(t)$-rational point of order 3 in $E(\mathbb{F}_q(t))$, we prove this adaptation by performing an elementary descent by 3-isogeny. In the end we look at explicit examples for the rank of an elliptic curve over a rational function field.

Keywords— Elliptic Curves, Function Fields, Mordell's Theorem, Descent by 3-Isogeny

Contents

1 Introduction

An important part of number theory is the study of so-called algebraic plane curves. An algebraic plane curve is defined by the zero set of a polynomial in two variables, which is defined over a field. It turns out that various problems in number theory can be reduced to the study of rational points on algebraic plane curves. In fact, when proving Fermat's Last Theorem, which states that no positive integers a, b and c exists such that $a^n + b^n = c^n$ for $n > 2$, Andrew Wiles used a very special family of algebraic plane curves, namely the elliptic curves [16]. These elliptic curves are algebraic plane curves defined by an equation of the form

$$E : y^2 = x^3 + ax^2 + bx + c, \tag{1.1}$$

where $f(x) := x^3 + ax^2 + bx + c$ has no multiple roots and the coefficients are from some field K with $\text{char}(K) \neq 2$. These type of curves turn out to carry a lot more structure than one would imagine by just looking at the equation that defines them. In fact, when considering the points on E with coordinates in K and adding an additional point at infinity one can construct a group denoted by $E(K)$.

Probably even less obvious is the fact that when $K = \mathbb{Q}$, the group of rational points on the curve E is finitely generated. A result proven by Louis Joel Mordell (28 January 1888 – 12 March 1972) in 1922 [7]. It turns out that this property holds in more generality. Approximately 30 years later S. Lang and A. Néron proved that the group of rational points on an abelian variety A over a field K is also finitely generated when K is finitely generated over its prime field [6]. This thesis will not discuss the full generality of abelian varieties. In fact, we will restrict ourselves to elliptic curves over rational function fields of the form $\mathbb{F}_q(t)$, where q is some prime power.

An important unsolved problem regarding the rank of $E(K)$, with K a number field, is the Birch and Swinnerton-Dyer conjecture [17]. It relates the rank of the group to an associated zeta function and it is one of the Millennium Prize Problems listed by the Clay Mathematics Institute. In fact, when considering the Birch and Swinnerton-Dyer conjecture over function fields a lot more is known [12, Section 2 & 3]. This makes the study of elliptic curves over function fields worthwhile. Moreover, the study of the rank is worthwhile, because the algebraic structure of the solution set of (1.1) is completely determined by the rank and the corresponding torsion group.

The main goal of this thesis is to show that the group of $\mathbb{F}_q(t)$-rational points on an elliptic curve over $\mathbb{F}_q(t)$ is finitely generated and to find a method for computing the rank. This result is a special case of the theorem by S. Lang and A. Néron, but we will prove it in an elementary way. To do so without having to resort to algebraic number theory over function fields we will make several extra assumptions along the way. One of them will be the existence of a $\mathbb{F}_q(t)$-rational point of order 3 on the curve, which will give us the tools to rewrite the equation of the curve in a more pleasant way. Some of the results proven hold for any rational function field $K(t)$ with $\text{char}(K)$ not 2 or 3. We will state in which cases theorems and lemmas hold in more generality than just for $\mathbb{F}_q(t)$.

We start by giving a short introduction on projective geometry and elliptic curves. After that we introduce the method of proof to show that $E(\mathbb{F}_q(t))$ is finitely generated, when there is a $\mathbb{F}_q(t)$-rational point of order 3 on the curve. In Sections 4 and 5 the theorem is proven and we end this thesis by considering some examples of elliptic curves and their rank.

2 Preliminaries

2.1 Projective Geometry and Curves

Before delving into the theory involving elliptic curves it is good to note that we are considering curves in the so-called projective plane and not in an affine space such as the Euclidean plane. This section is dedicated to give the appropriate background to study curves in the projective plane. We start by giving the definition of the K-rational points on the projective plane.

Definition 2.1. *Let K be a field. The set of K-rational points on the projective plane is defined as the set of triples $[a, b, c] \in K^3$, where we consider two triples to be equal if and only if they lie on the same line through the origin. In formal notation:*

$$\mathbb{P}^2(K) := \frac{\{[a, b, c] \colon a, b, c \in K \text{ not all zero}\}}{\sim},$$

where we say that two triples $[a, b, c] \sim [a', b', c']$ if and only if there is some nonzero t such that $[a, b, c] = [ta', tb', tc']$.

The projective plane seems to be a rather strange setting to study elliptic curves. However, it turns out to be incredibly useful to study these curves in $\mathbb{P}^2(K)$. Before we state this reason we first need the definition of the K-rational points on the affine plane.

Definition 2.2. *Let K be a field. The set of K-rational points on the affine plane is defined as*

$$\mathbb{A}^2(K) := \{(x, y) \colon x \text{ and } y \text{ are coordinates in } K\}.$$

As found in for example [9, Appendix A.1] we can associate $\mathbb{P}^2(K)$ with $\mathbb{A}^2(K)$ by adding all the directions in $\mathbb{A}^2(K)$ to $\mathbb{A}^2(K)$ itself. In other words, $\mathbb{P}^2(K) = \mathbb{A}^2(K) \cup \{\text{all directions in } \mathbb{A}^2(K)\}$. This means that we can view $\mathbb{P}^2(K)$ as $\mathbb{A}^2(K)$ with the addition of some extra points, which we call points at infinity. The addition of these points at infinity is important for the study of elliptic curves as it implies equality in Bézout's theorem [9, Appendix A.4]. This theorem asserts the existence of 3 intersection points of a cubic with a line, which we will need when creating a group structure on the elliptic curve.

Now that we have some intuition of the projective plane we can discuss the notion of a projective plane curve. We start by stating what it means for a polynomial to be homogeneous.

Definition 2.3. *Let K be a field. A polynomial $F(X, Y, Z) \in K[X, Y, Y]$ is called a homogeneous polynomial of degree d if it satisfies $F(tX, tY, tZ) = t^d F(X, Y, Z)$.*

With this definition we obtain the following notion of a projective plane curve C and its K-rational points.

Definition 2.4. *A projective plane curve C over a field K is defined by the set of solutions to*

$$F(X, Y, Z) = 0,$$

where $F(X, Y, Z) \in K[X, Y, Z]$ is a nonconstant homogeneous polynomial. We usually write this as $C \colon F(X, Y, Z) = 0$.

Definition 2.5. *Let K be a field and C be a projective plane curve. The set of K-rational points on C is the set*

$$C(K) := \{[X, Y, Z] \in \mathbb{P}^2(K) \colon F(X, Y, Z) = 0\}.$$

If we have a projective curve C we can define a new, nonhomogeneous, polynomial $f(x, y)$ by setting $f(x, y) := F(x, y, 1)$. We call $C_0 \colon f(x, y) = 0$ the affine part of a projective curve C. As completely discussed in [9, Appendix A.2] we can write any projective curve C as the union of its affine part C_0 together with its points at infinity (given by $Z = 0$). These points at infinity will correspond to the limiting directions of the tangent lines to the affine curve C_0. The process of reducing a projective plane curve C to an affine curve C_0 with some extra points at infinity is called dehomogenization. This process is not restricted to the variable Z, other affine points and other points at infinity can be obtained by for example setting $X = 1$ and $X = 0$. Note that for simplicity we usually write the curve in its affine form.

This process can also be done in reverse. If we start with a curve $C_0 \colon f(x, y) = 0$ in the affine plane, where $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$. Then we can get the corresponding projective plane curve $C \colon F(X, Y, Z) = 0$ by defining $F(X, Y, Z) := \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$, where d is the largest value of $i + j$ such that $a_{ij} \neq 0$.

Another important notion that is needed for the study of elliptic curves is the notion of singularity of projective plane curves. Before we say what this means, we first discuss the notion of singularity for affine curves.

Definition 2.6. *Let K be a field and let $C_0 \colon f(x, y) = 0$ be an affine plane curve over K. Let $P = (x, y)$ be a point on the curve C_0. We say that P is a singular point if*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

We call a point P on C_0 nonsingular if it is not singular and the curve C_0 is called nonsingular if every point on C_0 is nonsingular.

In a similar fashion the notion of singularity for a projective plane curve is given.

Definition 2.7. *Let K be a field and let $C \colon F(X, Y, Z) = 0$ be a projective plane curve over K. Let $P = [X, Y, Z]$ be a point on the curve C. We say that P is a singular point if*

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

We call a point P on C nonsingular if it is not singular and the curve C is called nonsingular if every point on C is nonsingular.

2.2 The Group Law on Elliptic Curves

As discussed before, Mordell's theorem states that the group of rational points on an elliptic curve over $\mathbb{Q}$ is finitely generated. This means that there is some sort of group theoretic structure on the rational points of an elliptic curve. This section is dedicated to the group law on elliptic curves. We start by giving the definition of an elliptic curve and a rational point on this curve. Note that we introduce the definition in its affine form due to the fact that in the upcoming sections we will mostly work with this form. Moreover, throughout this section (and throughout the rest of this thesis, unless specified otherwise) the field K is assumed to not have characteristic 2 or 3.

The reason for this assumption is quite delicate. If we allow characteristic 2, then the equation given in Definition 2.8 will not be general enough to describe all elliptic curves. Allowing

characteristic 3 would lead to issues in defining the 3-isogenies in Section 5.2, as $\bar{E}$ would not be a nonsingular curve in characteristic 3. For explicit p-descent in characteristic p, see [14].

Definition 2.8. *An elliptic curve over K is defined by a cubic equation*

$$E\colon y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in K$ and f has distinct roots, i.e., E is nonsingular.

We want the curve E to be nonsingular, because when defining the group law we need the existence of the derivative of f at every point on the curve E. In homogeneous form (so seen as a projective plane curve) the equation defining E becomes:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Setting $Z = 0$, we find $X^3 = 0$ and hence an elliptic curve has one point at infinity given by $(0 : 1 : 0)$, where $(0 : 1 : 0)$ denotes the equivalence class of the point $[0, 1, 0] \in \mathbb{P}^2(K)$. The point at infinity corresponds to the point where vertical lines meet, i.e., $x =$ "constant" in the affine plane. We call this point $\mathcal{O}$ and it will serve as the identity element of our group.

We know that a group is given by a triplet $(G, +, e)$, where G is a set, $+$ an operation and e the unit element. In the case of elliptic curves we have $G = E(K)$ and $e = \mathcal{O}$, where $E(K)$ denotes the set of K-rational points on E. The operation $+$, that makes this triplet into an abelian group is defined below.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be K-rational points on the elliptic curve. Draw a line through P and Q and call the third intersection point $P * Q$. Note that the existence of this third intersection point is always guaranteed due to equality in Bézout's theorem[†] and that it is K-rational by construction. To obtain $P + Q$ simply draw a vertical line through the point $P * Q$ (which is equivalent to joining $P * Q$ to $\mathcal{O}$), the point where this line intersects the curve is defined as $P + Q$. This process is seen in the figure below.

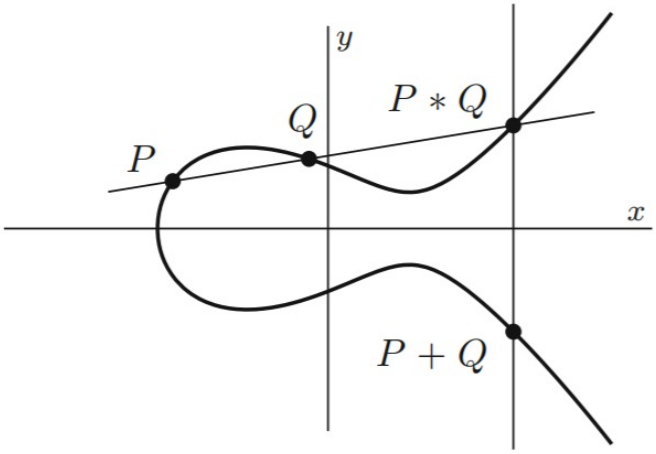

Figure 1: The group law on an elliptic curve [9, Section 1.4].

[†]Loosely speaking, equality in Bézout's theorem tells us that a straight line and a cubic curve always have three points of intersection, counting multiplicity, when seen as projective plane curves.

Note that there are some special cases; if we add the point P to itself, then the point $P * P$ is the intersection point with the curve and the tangent line through P. Also, if $P * Q$ is the point at infinity, then we obtain that $P + Q = \mathcal{O}$.

With this definition of the group law it becomes apparent that $P + Q = Q + P$, as the line connecting P to Q is the same as the line connecting Q to P and hence the group law is commutative. Moreover, the facts that the point at infinity $\mathcal{O}$ acts as the identity, that $+$ maps $E(K)$ to itself and that $P^{-1} = (x_1, -y_1)$ are also not hard to verify. Checking that the group law is associative is rather lengthy and hence skipped. For the interested reader we refer to [9, Section 1.4].

It is possible to deduce explicit formulas for this group law using tangent lines and lines through points. Deducing these formulas would not be very illuminating, hence we only state them. For the interested reader we again refer to [9, Section 1.4]. To get explicit formulas, let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $P * Q = (x_3, y_3)$. It is clear that $P + Q = (x_3, -y_3)$ and doing the computations we will obtain $x_3 = \lambda^2 - a - x_1 - x_2$ and $y_3 = \lambda x_3 + \nu$, where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1$.

As the observant reader might notice, these formulas are only valid if $P \neq Q$, i.e., the points P and Q need to be distinct. However, we would also like to be able to compute $P + P$ explicitly. Luckily, there is the so-called duplication formula. When we want to add the point $P = (x_1, y_1)$ to itself we need to use $\lambda = \frac{f'(x_1)}{2y_1}$ instead of $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. The rest of the formulas to compute x_3 and y_3 remain the same. Using this we can also obtain an explicit expression for the x-coordinate of $2(x, y)$. It is given as follows:

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}. \tag{2.1}$$

2.3 Points of Finite Order

In proving an analogue of Mordell's theorem over $\mathbb{F}_q(t)$ we will assume the existence of a rational point of order 3 on the elliptic curve. Due to this assumption it might not come as a surprise that points of order dividing 3 will play a major role in this thesis. Therefore, in this section, we will discuss more thoroughly the points of order 3 in $E(K)$.

Let P be a point of order 3 in $E(K)$, i.e., $3P = \mathcal{O}$ and $P \neq \mathcal{O}$. This is equivalent to saying $2P = -P$ and this tells us that $x(2P) = x(-P)$. Conversely, let $P \neq \mathcal{O}$ be such that $x(2P) = x(-P)$. As our curve E is symmetric around the x-axis we obtain that $2P = \pm P$. The assumption that $P \neq \mathcal{O}$ then tells us that $3P = \mathcal{O}$. We conclude that P is a point of order 3 in $E(K)$ if and only if $x(2P) = x(-P)$.

Write $P = (x, y)$ and consider the equation $x(2P) = x(-P)$. Using the duplication formula we can rewrite this equation as

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x.$$

Cross multiplying and combining terms implies that P is a point of order 3 if and only if the x-coordinate of P is a root of the polynomial $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$.

In Section 5 we will study elliptic curves of the form $E\colon y^2 = x^3 + A(x-B)^2$, where $A = a^2$ and B are in $\mathbb{F}_q[t]$. In this case a point P has order 3 in $E(\mathbb{F}_q(t))$ if and only if the x-coordinate of P is a root of

$$p_3(x) = 3x^4 + 4Ax^3 - 12ABx^2 + 12AB^2x. \tag{2.2}$$

Allowing points in the algebraic closure $\overline{\mathbb{F}_q(t)}$, we see that there are 8 points of order 3. Following [9, Theorem 2.1] we obtain that p_3 has four distinct roots and hence the group consisting of $\overline{\mathbb{F}_q(t)}$-rational points of order dividing 3 on E, denoted by $E(\overline{\mathbb{F}_q(t)})[3]$ and called the 3-torsion subgroup, is a group of order 9. All the elements have order dividing 3 and therefore $E(\overline{\mathbb{F}_q(t)})[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$. However, we would like to know how many points there are of order 3 that are $\mathbb{F}_q(t)$-rational. In any specific example we can deduce this using the rational root theorem.

Theorem 2.9 (The Rational Root Theorem)**.** *Let R be a unique factorization domain. Let $\mathrm{Frac}(R)$ be its field of fractions. Let $\frac{p}{q} \in \mathrm{Frac}(R)$, with $p, q \in R$ coprime, be a solution of a polynomial equation over R:*

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0.$$

Then q must divide a_n and p must divide a_0.

Proof. See [11, Section V.5] □

There are elliptic curves over $\mathbb{F}_q(t)$ that have $E(\mathbb{F}_q(t))[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$. For example, the curve $E\colon y^2 = x^3 + (4t^4 + 6t)x + (11t^6 + t^3 + 3)$ over $\mathbb{F}_{13}(t)$ has this property. When considering elliptic curves over $\mathbb{Q}$ this matter becomes less complicated. In fact, there can be at most three rational points of order 3 in $E(\mathbb{Q})$, as is found in [13, Section 2.4].

2.4 Isogenies of Elliptic Curves

This section contains a short introduction to the theory of isogenies and some useful results. We will not prove the results as they require knowledge about algebraic geometry and commutative algebra. An excellent reference on the rigorous theory of isogenies is [8, Sections III.4 & III.6]. The following definitions, lemmas and theorems are based on [15, Section 12].

Definition 2.10. *Let E_1 and E_2 be elliptic curves over a field K and let $\overline{K}$ be a fixed algebraic closure of K. An isogeny from E_1 to E_2 is a nonconstant group homomorphism $\phi\colon E_1(\overline{K}) \to E_2(\overline{K})$ that is given by rational functions.*

Important is that an isogeny is always a group homomorphism of K-rational points on E_1 to the K-rational points on E_2.

Lemma 2.11. *Let E_1 and E_2 be elliptic curves over a field K and let ϕ be an isogeny from E_1 to E_2. Then ϕ is of the form $\phi(x, y) = (r_1(x), yr_2(x))$, where r_1 and r_2 are rational functions.*

If the coefficients of the rational functions r_1 and r_2 lie in K, we say that the isogeny ϕ is defined over K.

Definition 2.12. *Keep the notation of Lemma 2.11 and write $r_1(x) = \frac{p(x)}{q(x)}$ with polynomials $p(x)$ and $q(x)$ that do not have a common factor. The degree of ϕ is defined as*

$$\deg(\phi) = \max\{\deg(p(x)), \deg(q(x))\}.$$

Definition 2.13. *Let E_1 and E_2 be elliptic curves over a field K. If ϕ is an isogeny from E_1 to E_2 of degree one, then we say that ϕ is an isomorphism of elliptic curves. In this case we say that E_1 is isomorphic to E_2.*

Definition 2.14. *Keep the notation of Lemma 2.11, we say that ϕ is separable if the derivative $r_1'(x)$ is not identically zero.*

Lemma 2.15. *Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves E_1 and E_2 that are defined over a field K. If ϕ is separable, then*

$$\deg(\phi) = \#\ker(\phi).$$

Theorem 2.16. *Let E_1 and E_2 be elliptic curves over a field K and let $\overline{K}$ be a fixed algebraic closure of K. Let $\phi\colon E_1(\overline{K}) \to E_2(\overline{K})$ be a nonconstant map given by rational functions. If $\phi(\mathcal{O}_1) = \mathcal{O}_2$, then ϕ is an isogeny.*

Theorem 2.17. *Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves that are defined over a field K. Then there exists a dual isogeny $\hat{\phi}\colon E_2 \to E_1$ such that $\hat{\phi} \circ \phi$ is multiplication by $\deg(\phi)$ on E_1.*

These results should give us enough information regarding isogenies to successfully deduce that the isogeny in Section 5 is in fact of degree 3.

The upcoming sections will discuss Mordell's theorem and its method of proof. In the next section we state and proof the so-called Descent theorem. The sections thereafter will be dedicated to proving the needed criteria for the Descent theorem.

3 Mordell's Theorem and Descent

Formally, Mordell's theorem can be stated as follows.

Theorem 3.1 (Mordell's Theorem)**.** *If E is an elliptic curve over $\mathbb{Q}$, then the group $E(\mathbb{Q})$ is finitely generated.*

In most introductory books Mordell's theorem is usually proved with the assumption that there exists a rational point of order 2 in $E(\mathbb{Q})$, because it makes the proof a lot simpler. Moreover, height functions and a descent method play an important role in the proof. We will use a similar approach for proving the main theorem of this thesis, which is as follows.

Theorem 3.2. *Let E be an elliptic curve over $\mathbb{F}_q(t)$ given by*

$$E\colon y^2 = x^3 + c \cdot A(x - B)^2,$$

where $A, B \in \mathbb{F}_q[t]$, $c \in \mathbb{F}_q$ and $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$. Moreover, assume that A is a perfect square in $\mathbb{F}_q(t)$. Then the group $E(\mathbb{F}_q(t))$ consisting of $\mathbb{F}_q(t)$-rational points on E is finitely generated.

Note that it is not strange to expect Mordell's theorem to hold over function fields of the form $\mathbb{F}_q(t)$. In fact, the fields $\mathbb{Q}$ and $\mathbb{F}_q(t)$ are quite similar. They are both the field of fraction of the Euclidean rings $\mathbb{Z}$ and $\mathbb{F}_q[t]$ respectively. Moreover, it turns out that $\mathbb{F}_q[t]$ has a similar distribution of irreducible elements as $\mathbb{Z}$, which makes them relatively similar in a number theoretic sense. For a closer look at the similarities, see [5].

Most of the needed lemmas to prove Theorem 3.2 can actually be proven for an arbitrary field K of characteristic not 2 or 3 instead of only for $\mathbb{F}_q$. Moreover, some properties can also

be proven for an arbitrary elliptic curve E of the form given in Definition 2.8. We will try to prove these lemmas in their most general form and only introduce extra constraints when necessary.

Theorem 3.2 can be proven using a so-called descent method, which is relatively similar to the method of infinite descent by Fermat [2]. The theorem holds for any abelian group and if we wish, we can completely forget that we are working with elliptic curves. The statement and proof follows [9, Theorem 3.5] and [13, Theorem 2]

Theorem 3.3 (The Descent Theorem)**.** *Let Γ be an abelian group and suppose that there exists a function (called a height function)*

$$h\colon \Gamma \to [0,\infty)$$

such that the following properties hold:

(1) For every real number M, the set $\{P \in \Gamma\colon h(P) \leq M\}$ is finite.
(2) For every $P_0 \in \Gamma$ there is a constant κ_0 so that

$$h(P+P_0) \leq 3h(P) + \kappa_0 \quad \text{for all } P \in \Gamma.$$

(3) There is a constant κ such that

$$h(3P) \geq 9h(P) - \kappa \quad \text{for all } P \in \Gamma.$$

Suppose further that
(4) The index $[\Gamma\colon 3\Gamma]$ is finite, where $3\Gamma := \{g \in \Gamma\colon g = 3g' \text{ for some } g' \in \Gamma\}$.

Then the group Γ is finitely generated.

One should remark a few things. The first one being that all four criteria of the Descent theorem are necessary to conclude that the group is finitely generated. For example, the additive group $\mathbb{Q}$ is not finitely generated, but $[\mathbb{Q}\colon 3\mathbb{Q}] = [\mathbb{Q}\colon \mathbb{Q}] = 1$. Moreover, the particular choice of the numbers 3 and 3^2 is not special at all. In fact, this theorem can be proven for any integer m as is done in [8, Section VIII.3]. With this being said we prove the Descent theorem.

Proof of the Descent Theorem. As $[\Gamma\colon 3\Gamma]$ is finite, we have that there are finitely many points that represent the cosets of 3Γ in Γ, and we call them $Q_1, \dots, Q_n$. If P is an arbitrary element in Γ, then it must live in one of the cosets $Q_1, \dots, Q_n$. In other words, there is some index i_1 and element $P_1 \in \Gamma$ such that

$$P = 3P_1 + Q_{i_1}.$$

This process can be repeated inductively and we obtain the following:

$$\begin{aligned} P_1 &= 3P_2 + Q_{i_2}, \\ P_2 &= 3P_3 + Q_{i_3}, \\ &\vdots \\ P_{m-1} &= 3P_m + Q_{i_m}, \end{aligned}$$

where $Q_{i_1}, \dots, Q_{i_m}$ are chosen from the representatives $Q_1, \dots, Q_n$ and $P_1, \dots, P_m \in \Gamma$. Note that from the first two equations we can write

$$P = 3(3P_2 + Q_{i_2}) + Q_{i_1} = 3^2 P_2 + 3Q_{i_2} + Q_{i_1}.$$

Applying all the equations obtained above will eventually give us the following expression for P:

$$P = Q_{i_1} + 3Q_{i_2} + 3^2 Q_{i_3} + \cdots + 3^{m-1} Q_{i_m} + 3^m P_m.$$

In particular, this tells us that $P \in \langle Q_{i_1}, \ldots, Q_{i_m}, P_m \rangle$; the subgroup of Γ generated by the $Q_{i_1}, \ldots, Q_{i_m}$ and P_m. As $\{Q_{i_1}, \ldots, Q_{i_m}\}$ is a subset of the set of all the cosets of 3Γ in Γ we can in fact say that $P \in \langle Q_1, \ldots, Q_n, P_m \rangle$.

Our goal now is to show that P_m can be chosen from a finite set, as that would indeed imply that Γ is finitely generated. So far we have only used the fact that $[\Gamma : 3\Gamma]$ is finite, but we also need to use the other 3 properties stated in the theorem. In fact, using property (2) we obtain that

$$h(P - Q_i) \leq 3h(P) + \kappa_i,$$

for some κ_i independent of P and all $i = 1, \ldots, n$. Defining $\kappa' := \max\{\kappa_i\}$ we obtain that $h(P - Q_i) \leq 3h(P) + \kappa'$ for all $i = 1, \ldots, n$. If we now apply property (3) we get the following:

$$\begin{aligned} 9h(P_j) &\leq h(3P_j) + \kappa \\ &= h(P_{j-1} - Q_{i_j}) + \kappa \\ &\leq 3h(P_{j-1}) + \kappa + \kappa'. \end{aligned}$$

Dividing both sides by 9 and rearranging some terms yields that

$$h(P_j) \leq \frac{4}{9} h(P_{j-1}) - \frac{1}{9} \left(h(P_{j-1}) - (\kappa + \kappa') \right).$$

If $h(P_{j-1}) \geq \kappa + \kappa'$, then we have $h(P_j) \leq \frac{4}{9} h(P_{j-1})$. From this we can conclude that the sequence of P_j's is such that $h(P_j) \to 0$ and hence there will be some index m for which $h(P_m) \leq \kappa + \kappa'$. We can pick this index and subsequently find that $P \in \langle Q_1, \ldots, Q_n, P_m \rangle$, where $h(P_m) \leq \kappa + \kappa'$. We conclude that Γ is generated by $\{Q_1, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\}$. From property (1) we know that this is in fact a finite set, which finishes the proof. □

The following sections will mainly be focussed on applying the Descent theorem to prove Theorem 3.2. Most of the upcoming results are straightforward results from either [18] or [13] and we will only give some outline of the ideas. For full rigorous proofs one should refer to the aforementioned theses.

4 Heights on Function Fields

To prove Mordell's theorem one defines a so-called height function h on the rational numbers. It turns out that this function is precisely the function that satisfies the first three properties of the Descent theorem. We want to define a similar function, but then for the field $\mathbb{F}_q(t)$ instead of $\mathbb{Q}$. Before doing this we first look at the definition of the height of a rational number.

Definition 4.1. *The height of a rational number is given by the function $h : \mathbb{Q} \to \mathbb{R}_{\geq 0}$, which is defined by $h(x) := \log \max\{|m|, |n|\}$ and where $x = \frac{m}{n}$ is written in lowest terms.*

Two things should get our attention in this definition. The first one being the notion of the absolute value of an integer and the second one being the fact that $h(x)$ sort of tells us something about the complexity of x. For example the height of $\frac{1}{2}$ is much smaller than the height of $\frac{500}{1001}$,

although the numbers are very close to each other on the number line.

To obtain a height function h on $\mathbb{F}_q(t)$ we will first define a absolute value on $\mathbb{F}_q[t]$. In fact, most of the upcoming results work for any field K with $\mathrm{char}(K)$ not 2 or 3.

Definition 4.2. *The function $|\cdot|\colon K[t] \to \mathbb{R}_{\geq 0}$ is said to be an absolute value on $K[t]$ if it satisfies the following properties:*

(1) $|f| \geq 0$ *for all* $f \in K[t]$*, with equality if and only if* $f = 0$*,*
(2) $|fg| = |f||g|$ *for all* $f, g \in K[t]$*,*
(3) $|f + g| \leq |f| + |g|$*.*

One can easily check that the function $|f| := e^{\deg(f)}$ is an absolute value on $K[t]$ if we set $\deg(0) = -\infty$. Moreover, if $K = \mathbb{F}_q$, then also the function $|f| := q^{\deg(f)}$ works as an absolute value. We are now ready to define a height function on the rational function field $K(t)$.

Definition 4.3. *The function $h\colon K(t) \to \mathbb{R}_{\geq 0}$ defined by $h(x(t)) = \max\{\deg(f), \deg(g)\}$, where $x(t) = \frac{f(t)}{g(t)}$ is written in lowest terms, is called the height of $x(t)$.*

We should note that the definition of height on $K(t)$ is defined analogously to the height function on $\mathbb{Q}$. This follows from the following:

$$h(x(t)) = \max\{\deg(f), \deg(g)\} = \max\{\log|f|, \log|g|\} = \log\max\{|f|, |g|\}.$$

To be able to apply the Descent theorem to the abelian group $E(\mathbb{F}_q(t))$ we need the notion of height of a point on $E(\mathbb{F}_q(t))$, however this is simply defined as the height of its x-coordinate. Formally stated:

Definition 4.4. *Let $P = (x(t), y(t))$ be a point on an elliptic curve over $\mathbb{F}_q(t)$. The height of P is defined as $h(P) := h(x(t))$ and if $P = \mathcal{O}$, then we define $h(\mathcal{O}) = 0$.*

Our ultimate goal is to prove that $E(\mathbb{F}_q(t))$ is finitely generated. We will systematically follow the steps of the Descent theorem, which we will state as four consecutive lemmas for convenience.

Lemma 4.5. *For every real number M, the set*

$$\{P \in E(\mathbb{F}_q(t))\colon h(P) \leq M\}$$

is finite.

Lemma 4.6. *For every $P_0 \in E(\mathbb{F}_q(t))$ there is a constant κ_0 so that*

$$h(P + P_0) \leq 3h(P) + \kappa_0 \quad \text{for all } P \in E(\mathbb{F}_q(t)).$$

Lemma 4.7. *There is a constant κ such that*

$$h(3P) \geq 9h(P) - \kappa \quad \text{for all } P \in E(\mathbb{F}_q(t)).$$

Lemma 4.8. *The index $[E(\mathbb{F}_q(t))\colon 3E(\mathbb{F}_q(t))]$ is finite.*

The first three lemmas are the easiest to prove and can be done for any elliptic curve E defined over $\mathbb{F}_q(t)$. The fourth lemma will be proven with the curve E from Theorem 3.2 and the extra assumptions stated in that theorem to avoid algebraic number theory over function fields. We start by giving the proof of Lemma 4.5.

Proof of Lemma 4.5. Note that it suffices to show that the number of elements in

$$\mathcal{Z} := \{x \in \mathbb{F}_q(t) \colon h(x) \leq M\}$$

is finite for all $M \geq 0$. This follows from the fact that the set of x-coordinates of $\mathbb{F}_q(t)$-rational points on E with bounded height is subset of $\mathcal{Z}$ and for each x-coordinate we have at most two y-coordinates. So we take an arbitrary $x \in \mathcal{Z}$ and write it in lowest terms as $x = \frac{f(t)}{g(t)}$, where f and g are in $\mathbb{F}_q[t]$. Since f and g are polynomials over a finite field with q elements and their degree is bounded due to x being in $\mathcal{Z}$, we can conclude that there are only finitely many possibilities for the polynomials f and g. Hence there are also only finitely many possibilities for the element x, which concludes the proof. □

During this thesis we try to keep things as general as possible, with regard to which field we take for K in $E(K(t))$. One should realize that the proof of Lemma 4.5 only works for finite fields K. For example, if one would consider the set

$$\{x \in \mathbb{R}(t) \colon h(x) \leq M\},$$

then it becomes clear that this set is not finite for all $M > 0$ as there are already infinitely many polynomials of degree 1 in $\mathbb{R}(t)$.

Before we can prove Lemma 4.6 we need to achieve some auxiliary results. We will state them as lemmas and use them in the proof of Lemma 4.6. Again, most of these results hold for any elliptic curve E and any field K with $\mathrm{char}(K)$ not 2 or 3.

Lemma 4.9. *Let $P = (x, y)$ be a point on an elliptic curve E with $x, y \in K(t)$. We can write $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$, where $m, n, e \in K[t]$, $e \neq 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.*

Proof. This is just a slight adaptation of the proof given in [9, Section 3.2], where we should keep in mind that we are working over $K(t)$ and not over $\mathbb{Q}$. For the full proof the reader should look at [18, Section 4.3]. □

There is one more lemma needed before we can prove Lemma 4.6, which is stated below.

Lemma 4.10. *Let $P = (x, y)$ be a point on an elliptic curve E with $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$, where $m, n, e \in K[t]$, $e \neq 0$ and $\gcd(m, e) = \gcd(n, e) = 1$. Then we have that*

$$\deg(n) \leq k + \frac{3}{2} h(P),$$

for some constant k depending on a, b and c.

Proof. The idea of the proof is as follows. First of all we should note that the following two properties hold for elements $f, g \in K[t]$:

(1) $\deg(fg) = \deg(f) + \deg(g)$,
(2) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

Moreover, both $\deg(e^2)$ and $\deg(m)$ are less than or equal to $h(P)$. These (in)equalities will give an upper bound for $\deg(n^2)$.

The point P is assumed to be a rational point on the curve E. Hence we can plug in the point into the equation of the curve E and by clearing denominators we obtain the following equation:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6. \tag{4.1}$$

Using equation (4.1) and the aforementioned inequalities yields $\deg(n) \leq k + \frac{3}{2}h(P)$, where $k := \frac{1}{2}\max\{\deg(a), \deg(b), \deg(c)\}$. For a more detailed version of the proof, see [18, Proposition 2] □

We now have the appropriate tools to prove Lemma 4.6. In contrast to the proof of Lemma 4.5 where K needs to be a finite field, this proof works for a general field with characteristic not 2 or 3.

Proof of Lemma 4.6. Again, we will only give an outline of the proof. A more detailed version is available in [18, Lemma 2]. First of all, note that we can exclude any fixed finite set of points P. This follows from the fact that for any finite number of points P, we just look at the differences $h(P + P_0) - 3h(P)$ and take κ_0 larger than the finite number of values that occur. Having said this we proof the statement for $P \notin \{P_0, -P_0, \mathcal{O}\}$ as we can then avoid using the duplication formula. In fact, the additional assumption of $P_0 \neq \mathcal{O}$ can be made, because the inequality would be trivial in this case.

Write $P = (x, y)$, $P_0 = (x_0, y_0)$ and $P + P_0 = (\xi, \eta)$. The goal is to write $h(P + P_0) = h(\xi)$ in terms of $h(P) = h(x)$. Using the formulas from the group law as found in Section 2.2 we have the following expression for ξ:

$$\xi = \lambda^2 - a - x - x_0 \quad \text{with } \lambda = \frac{y_0 - y}{x_0 - x}. \tag{4.2}$$

Some computations and recalling that any rational point (x, y) on E can be written as $(\frac{m}{e^2}, \frac{n}{e^3})$ yields that

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4},$$

where $A, \ldots, G$ are certain elements in $K(t)$ depending on a, b, c, x_0 and y_0. We do not know whether this in written in lowest terms, but in any case we can write

$$h(\xi) \leq \max\{\deg(Ane + Bm^2 + Cme^2 + De^4), \deg(Em^2 + Fme^2 + Ge^4)\}.$$

We are now left with two cases, the first one is when this maximum equals $\deg(Ane + Bm^2 + Cme^2 + De^4)$ and the second one when this maximum equals $\deg(Em^2 + Fme^2 + Ge^4)$. Using Lemma 4.10 we obtain in the first case that

$$h(\xi) \leq \max\{\deg(A) + k, \deg(B), \deg(C), \deg(D)\} + 2h(P)$$

and in the second case that

$$h(\xi) \leq \max\{\deg(E), \deg(F), \deg(G)\} + 2h(P).$$

Defining $\kappa_0 := \max\{\deg(A) + k, \deg(B), \deg(C), \deg(D), \deg(E), \deg(F), \deg(G)\}$ shows that $h(\xi) \leq 2h(P) + \kappa_0$ and hence also $h(\xi) \leq 3h(P) + \kappa_0$, as desired. □

We are now halfway through proving that $E(\mathbb{F}_q(t))$ is finitely generated. We have already shown that our function h satisfies the first and second condition for the Descent theorem. This section finishes by showing the third property of h that is needed for the descent argument. Section 5 will show that the index $[E(\mathbb{F}_q(t)) : 3E(\mathbb{F}_q(t))]$ is finite.

Before we continue it is convenient to introduce some new notation. We define the function $H : K(t) \to \mathbb{R}_{\geq 0}$ as $H(x) = e^{h(x)}$ (or $e = q$ in case of K being finite). Note that this function H is nothing more than raising the function h from Definition 4.3 to the power e (or q). The following lemma concerned with the function H is tremendously useful.

Lemma 4.11. *Let $\phi(X)$ and $\psi(X)$ be coprime in $K(t)[X]$ and let $d = \max\{\deg(\phi), \deg(\psi)\}$. Then there exists a positive constant C such that*

$$CH(x)^d \leq H\left(\frac{\phi(x)}{\psi(x)}\right) \quad \text{for all } x \in K(t).$$

Proof. The proof of this theorem has nothing to do with elliptic curves and hence we refer to [18, Section 4.4] for the full proof. □

The use of Lemma 4.11 only shows itself when we know something about the point $3P$ on the curve E. In fact, if we have a rational point $P = (x, y)$ on E and the point $3P = (\xi, \eta)$, we would like to show that ξ is a quotient of coprime polynomials $\phi(X)$ and $\psi(X)$ in $K(t)[X]$ with $\max\{\deg(\phi), \deg(\psi)\} = 9$. Taking logarithms of the equation in Lemma 4.11 then yields that $h(\xi) \geq 9h(x) - \log(C)$ for all $x \in K(t)$. All of this implies that $h(3P) \geq 9h(P) - \log(C)$, which proves Lemma 4.7.

We formally state the aforementioned property of ξ and refer to the proof.

Proposition 4.12. *Let $P = (x, y)$ be a rational point on the curve E and write (ξ, η) for the point $3P$. The coordinate ξ can be written as a quotient of two coprime polynomials $\phi(X)$ and $\psi(X)$ in $K(t)[X]$, with $\max\{\deg(\phi), \deg(\psi)\} = 9$.*

Proof. The proof of this statement is very tedious and is done in [13, Appendix B]. The proof of the case $K(t)$ is completely similar. A similar result even holds for multiplication by any integer n, not only for $n = 3$. The interested reader is referred to [15, Section 3.2], where some theory on division polynomials is discussed. □

As explained before, we have now in fact shown Lemma 4.7. Hence we have treated all the properties regarding heights for the descent argument. Next section will be dedicated completely to showing that the index is finite. In order to do so without having to resort to topics as algebraic number theory over function fields or Galois cohomology we have to make some extra assumptions.

5 Bounding the Index

In this section we will prove that the index $[E(L)\colon 3E(L)]$ is finite, where $L := \mathbb{F}_q(t)$ and $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$. We will not do this for a general elliptic curve E, but we will do this for elliptic curves of the form

$$E\colon y^2 = x^3 + A(x - B)^2,$$

where the coefficients A and B are from $\mathbb{F}_q[t]$ and A is a perfect square. We will later see that this result helps us in proving Theorem 3.2. This choice for the curve E is not completely arbitrary. In fact, we will show that any elliptic curve having an L-rational point of order 3 can be written in this form.

5.1 Rewriting the Elliptic Curve

Let $P = (\alpha, \beta)$ be a L-rational point of order 3 on an elliptic curve given by $E : y^2 = x^3 + ax^2 + bx + c$. Shifting the x-coordinate of P to 0, i.e., replacing x by $x + \alpha$ gives us the following:

$$\begin{aligned} y^2 &= (x + \alpha)^3 + a(x + \alpha)^2 + b(x + \alpha) + c \\ &= x^3 + x^2(3\alpha + a) + x(3\alpha^2 + 2a\alpha + b) + \alpha^3 + a\alpha^2 + \alpha b + c \\ &= x^3 + x^2(3\alpha + a) + x(3\alpha^2 + 2a\alpha + b) + \beta^2. \end{aligned}$$

Renaming $3\alpha + a$ to a and $3\alpha^2 + 2a\alpha + b$ to b gives an equation of the form:

$$y^2 = x^3 + ax^2 + bx + \beta^2.$$

The point $(0, \beta)$ is of order 3, hence we have $2(0, \beta) = (0, -\beta)$. Using the duplication formula we obtain that $\left(\frac{b^2-4a\beta^2}{4\beta^2}, \frac{4ab\beta^2-b^3-8\beta^4}{-8\beta^3}\right) = (0, -\beta)$ and hence $b^2 = 4a\beta^2$. Suppose that $b \neq 0$[†], then $a \neq 0$ and a must be a perfect square. All of this means that there is an element $z \in \mathbb{F}_q(t)$ such that $z^2 = \frac{\beta^2}{a}$. Combining everything yields the following equation:

$$\begin{aligned} y^2 &= x^3 + ax^2 + \sqrt{4a^2z^2}x + z^2a \\ &= x^3 + ax^2 + 2azx + z^2a \\ &= x^3 + a(x + z)^2. \end{aligned}$$

Let us write $z = \frac{f}{g}$, then we multiply the obtained equation by g^6 and obtain

$$(yg^3)^2 = (xg^2)^3 + ag^2(xg^2 + fg)^2.$$

Changing coordinates $y := yg^3$ and $x := xg^2$ yields that the equation can be written as

$$y^2 = x^3 + d(x + r)^2,$$

for some perfect square $d \in \mathbb{F}_q(t)$ and $r \in \mathbb{F}_q[t]$. Write $d = \frac{w^2}{t^2}$ in lowest terms and multiply the equation by t^6 to obtain

$$y^2t^6 = x^3t^6 + w^2(xt^2 + rt^2)^2.$$

Changing coordinates as before yields that the equation can be written as

$$y^2 = x^3 + w^2(x + rt^2)^2,$$

with w^2 and rt^2 both in $\mathbb{F}_q[t]$. Setting $A := w^2$ and $B := -rt^2$ shows indeed that the curve can be written as

$$E : y^2 = x^3 + A(x - B)^2, \tag{5.1}$$

with A a perfect square and B both in $\mathbb{F}_q[t]$. This justifies the study of elliptic curves of this form.

5.2 The Curve $\bar{E}$ and the Homomorphisms ϕ and $\hat{\phi}$

Showing that $[E(L) \colon 3E(L)] < \infty$ is the hardest part in showing that $E(L)$ is finitely generated. The statement is similar to a theorem known as the weak Mordell-Weil theorem, which states that $[E(K) \colon mE(K)]$ is finite for any elliptic curve E over K and integer m, where K a number field (a finite extension of $\mathbb{Q}$). M. van Beek shows in [13] that $[E(\mathbb{Q}) \colon 3E(\mathbb{Q})]$ is finite for elliptic curves over $\mathbb{Q}$ of the form $E \colon y^2 = x^3 + A(x - B)^2$, where A is not necessarily a perfect square. We try to adapt her proof to elliptic curves over function fields. Before stating the outline of the proof, first some notation.

Definition 5.1. *Let K be a field. The group of units of K is denoted by K^*. Moreover, we define $K^{*3} := \{\beta \in K^* \colon \beta = \gamma^3$ for some $\gamma \in K^*\}$.*

[†]See Section 7 for the case $b = 0$.

We will prove that the index is finite by considering the following two points.

1. First we will introduce another elliptic curve $\bar{E}$ over L and two homomorphisms $\phi : E(L) \to \bar{E}(L)$ and $\hat{\phi} : \bar{E}(L) \to E(L)$. These mappings will turn out to satisfy $\hat{\phi} \circ \phi = [3]$, where $[3]$ stands for multiplication by 3 in $E(L)$. These mappings are obtained from [3, Section 8.4].
2. After the introduction of this new curve $\bar{E}$ we will introduce two group homomorphisms $\alpha \colon E(L) \to L^*/L^{*3}$ and $\bar{\alpha} \colon \bar{E}(L) \to L^*/L^{*3}$. These mappings will provide a way to bound the index.

From Section 5.1 we know that A is a perfect square, i.e., $A = a^2$ for some $a \in \mathbb{F}_q[t]$. In fact, because we will define a similar map $\bar{\alpha}$ we will also assume that -3 is a square in L. This is for example the case when $q \in \{7, 13, 19\}$. For such q we will denote $\delta := \sqrt{-3} \in L$. As we will see later, the assumption that -3 is a perfect square is not necessary. However, this assumption will simplify things a lot in the upcoming statements. We now give explicit equations for the curve $\bar{E}$ and the mapping ϕ. The curve $\bar{E}$, found in [3, Section 8.4], is given by:

$$\bar{E} \colon y^2 = x^3 + \bar{A}(x - \bar{B})^2, \tag{5.2}$$

where $\bar{A} = -3A = \delta^2 a^2$ and $\bar{B} = \frac{4A+27B}{9}$. The mapping ϕ is given by:

$$\begin{aligned} \phi \colon E(\overline{L}) &\to \bar{E}(\overline{L}) \\ (x, y) &\mapsto (\xi, \eta), \end{aligned} \tag{5.3}$$

where $\xi = \frac{1}{x^2}\left(x^3 + 4A\left(\frac{1}{3}x^2 - Bx + B^2\right)\right)$, $\eta = \frac{y}{x^3}\left(x^3 + 4AB\left(x - 2B\right)\right)$ and $\overline{L}$ denotes a fixed algebraic closure of L.

Following [3, Section 8.4] we have that $\phi(\mathcal{O}) = \phi(0, \pm aB) = \bar{\mathcal{O}}$, so that $\ker(\phi) = \{\mathcal{O}, (0, \pm aB)\}$. Theorem 2.16 then tells us that ϕ is an isogeny and Theorem 2.17 tells us that there exists a dual isogeny $\hat{\phi}$ such that $\hat{\phi} \circ \phi$ is multiplication by $\deg(\phi)$ on E. This dual isogeny is given by:

$$\begin{aligned} \hat{\phi} \colon \bar{E}(\overline{L}) &\to E(\overline{L}) \\ (\xi, \eta) &\mapsto (x, y), \end{aligned} \tag{5.4}$$

where $x = \frac{1}{9\xi^2}\left(\xi^3 + 4\bar{A}(\frac{1}{3}\xi^2 - \bar{B}\xi + \bar{B}^2)\right)$, $y = \frac{\eta}{27\xi^3}\left(\xi^3 + 4\bar{A}\bar{B}(\xi - 2\bar{B})\right)$ and $\hat{\phi}(\bar{\mathcal{O}}) = \hat{\phi}(0, \pm\delta a\bar{B}) = \mathcal{O}$. In fact, due to Definition 2.14 it is not hard to see that ϕ is separable and hence by Lemma 2.15 we have that $\deg(\phi) = 3$. Therefore we have that $\hat{\phi} \circ \phi$ is just multiplication by 3 in $E(L)$, as the isogenies ϕ and $\hat{\phi}$ restrict to group homomorphisms when considered as mappings from $E(L) \to \bar{E}(L)$ and $\bar{E}(L) \to E(L)$ respectively.

The introduction of the curve $\bar{E}$ and the homomorphisms ϕ and $\hat{\phi}$ is not without reason. The fact that multiplication by 3 on E can be split into two homomorphism is very convenient as the following proposition explains.

Proposition 5.2. *Let A and B be abelian groups and suppose that $\phi \colon A \to B$ and $\hat{\phi} \colon B \to A$ are homomorphisms satisfying $\hat{\phi} \circ \phi = [n]$, where $[n]$ denotes multiplication by $n \in \mathbb{Z}_{\geq 2}$ on the group A. Moreover, suppose that $\phi(A)$ has finite index in B and that $\hat{\phi}(B)$ has finite index in A. Then*

$$[A \colon nA] \leq [A \colon \hat{\phi}(B)][B \colon \phi(A)].$$

Proof. Write $b_1, \cdots, b_m$ for the cosets of $\phi(A)$ in B and $a_1, \cdots, a_l$ for the cosets of $\hat{\phi}(B)$ in A. We claim that the cosets of nA in A can all be represented by elements from

$$\mathcal{C} := \{a_i + \hat{\phi}(b_j) \colon 1 \leq i \leq l, 1 \leq j \leq m\}.$$

The above statements implies that we need to show that any $a \in A$ can be written as an element of some coset $\beta + nA$, where $\beta \in \mathcal{C}$. In other words, we need to show that $a = \beta + na'$ for some $a' \in A$. So take an arbitrary element $a \in A$. As a must be in one of the cosets of $\hat{\phi}(B)$ in A we can write $a = a_i + \hat{\phi}(b)$ for some representative a_i and some $b \in B$. Similarly we can write $b = b_j + \phi(a')$ for some representative b_j and some element $a' \in A$. Using this we can write:

$$\begin{aligned} a &= a_i + \hat{\phi}(b) \\ &= a_i + \hat{\phi}(b_j + \phi(a')) \\ &= a_i + \hat{\phi}(b_j) + na', \end{aligned}$$

which shows that $\mathcal{C}$ contains a complete set of cosets for nA in A. As $\mathcal{C}$ has at most mn elements, the statement follows. □

Returning to the realm of elliptic curves, where we want to show that $[E(L) \colon 3E(L)] < \infty$, we see that Proposition 5.2 is extremely useful. In fact, because we have already established that multiplication by 3 on E can be decomposed into 2 homomorphisms ϕ and $\hat{\phi}$, we only need to show that both $[E(L) \colon \hat{\phi}(\bar{E}(L))]$ and $[\bar{E}(L) \colon \phi(E(L))]$ are finite, as Proposition 5.2 with $n = 3$ then shows that $[E(L) \colon 3E(L)]$ is finite.

5.3 The Group Homomorphism α

To show the indices are $[E(L) \colon \hat{\phi}(\bar{E}(L))]$ and $[\bar{E}(L) \colon \phi(E(L))]$ finite, a map $\alpha \colon E(L) \to L^*/L^{*3}$ will be introduced. The definition of α is adapted from [3, Definition 8.4.7] and it is given as:

$$\alpha(P) = \begin{cases} \overline{1}, & \text{if } P = \mathcal{O}, \\ \overline{y - (x - B)a}, & \text{if } P = (x, y) \in E(L), \end{cases} \tag{5.5}$$

where $\overline{d} := d \bmod L^{*3}$ for some $d \in L^*$.

It will be shown that α is a homomorphism with finite image. Moreover, it will be shown that $\ker(\alpha) = \hat{\phi}(\bar{E}(L))$, where $\hat{\phi}$ is seen as a group homomorphism between rational points on elliptic curves. This means by the first isomorphism theorem that $E(L)/\hat{\phi}(\bar{E}(L)) \cong \alpha(E(L))$ and because α has finite image we can conclude that $[E(L) \colon \hat{\phi}(\bar{E}(L))]$ is finite. This of course does not show that the other index is finite, however we can define a map $\bar{\alpha} \colon \bar{E}(L) \to L^*/L^{*3}$ analogously to α (as -3 is a perfect square in L) and from that obtain that the other index is finite as well. Using this it suffices to show that α is a homomorphism with finite image and $\ker(\alpha) = \hat{\phi}(\bar{E}(L))$.

As the observant reader might notice, the map α is not properly defined yet. Namely, if $y - (x - B)a = 0$, then the map α is not defined. Luckily this only happens for points of the form $\pm P = (0, \pm aB)$. We define α for these points separately: $\alpha(0, aB) := \overline{2aB}$ and $\alpha(0, -aB) := \overline{\frac{1}{2aB}}$. Now that α is properly defined, it will be shown that it is a homomorphism. This will be done in two steps, which will be stated as lemmas.

Lemma 5.3. *The map α sends inverses to inverses. In other words:*

$$\alpha(-P) = \alpha(P)^{-1}.$$

Proof. The statement is clear for $P = \mathcal{O}$ and $P = (0, \pm aB)$. In all other cases $x \neq 0$ and for the point $P = (x, y)$ we obtain:

$$\begin{aligned}
\alpha(P)^{-1} &\equiv \frac{1}{y - (x - B)a} \pmod{L^{*3}} \\
&\equiv \frac{y + (x - B)a}{x^3} \pmod{L^{*3}} \\
&\equiv y + (x - B)a \pmod{L^{*3}} \\
&\equiv -y - (x - B)a \pmod{L^{*3}} \\
&\equiv \alpha(-P),
\end{aligned}$$

where in the second equality we used that $x^3 = (y + (x - B)a)(y - (x - B)a)$. □

Lemma 5.4. *Let P_1, P_2 and P_3 be L-rational points on E. If $P_1 + P_2 + P_3 = \mathcal{O}$, then $\alpha(P_1)\alpha(P_2)\alpha(P_3) = \overline{1}$.*

Proof. There are a few trivial cases of this lemma such as $P_1 = P_2 = P_3 = \mathcal{O}$ and $P_1 = (0, aB), P_2 = (0, -aB), P_3 = \mathcal{O}$. It is not hard to see that the statement holds for these cases. We turn towards the nontrivial case.

From [9, Section 1.4] we know that having three L-rational points on E summing to $\mathcal{O}$ is equivalent to saying that they are colinear. Write $y = \lambda x + \nu$ for the line through P_1, P_2 and P_3, and write x_1, x_2, x_3 for the x-coordinates of the points P_1, P_2, P_3 respectively. Plugging in $y = \lambda x + \nu$ into the equation of the elliptic curve gives:

$$x^3 + (A - \lambda^2)x^2 + (-2AB - 2\lambda\nu)x + AB^2 - \nu^2 = 0.$$

We know that x_1, x_2 and x_3 are the roots of this polynomial, hence we have the following expressions for the x_i:

$$\begin{aligned}
x_1 + x_2 + x_3 &= \lambda^2 - A, \\
x_2x_3 + x_1x_2 + x_1x_3 &= -2(AB + \lambda\nu), \\
x_1x_2x_3 &= \nu^2 - AB^2.
\end{aligned} \tag{5.6}$$

Writing out $\alpha(P_1)\alpha(P_2)\alpha(P_3)$ with the definition of α and using the equations from (5.6) to rewrite the expression we find that

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = (\nu + aB)^3.$$

The explicit calculations of this result are very tedious and can be found in [13, Section 3.2][†]. Using this we see that $\alpha(P_1)\alpha(P_2)\alpha(P_3)$ is a perfect cube and hence $\alpha(P_1)\alpha(P_2)\alpha(P_3) = \overline{1}$, as desired. □

Showing α is a homomorphism is now very easy.

Theorem 5.5. *The mapping α given by (5.5) is a homomorphism.*

[†]The result proven there is the same as ours up to sign.

Proof. From Lemma 5.3 and Lemma 5.4 we see the following:

Let P_1 and P_2 be rational points on E and let P_3 be the third intersection with the line through P_1, P_2 and E. Then we have

$$\begin{aligned}\alpha(P_1 + P_2) &= \alpha(-P_3)\\ &= \alpha(P_3)^{-1}\\ &= \alpha(P_1)\alpha(P_2),\end{aligned}$$

which shows that α is indeed a homomorphism. □

What remains to be shown is that α has finite image and that $\ker(\alpha) = \hat{\phi}(\bar{E}(L))$. We fill now first show that α has finite image, which is a rather straightforward adaptation of [13, Section 4.1]

Theorem 5.6. . *The image of the mapping α from (5.5) is contained in the subgroup of L^*/L^{*3} consisting of elements $\{up_1^{\epsilon_1}\cdots p_j^{\epsilon_j}\}$, where $\epsilon_i \in \{0,1,2\}$, $u \in \mathbb{F}_q^*/\mathbb{F}_q^{*3}$ and the p_i are monic irreducible elements that divide $2aB$.*

Proof. From Lemma 4.9 we know that we can write $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ with $\gcd(m,e) = \gcd(n,e) = 1$ and $e \neq 0$. Plugging these values for x and y into the equation for E and clearing denominators yields

$$n^2 = m^3 + a^2m^2e^2 - 2a^2Bme^4 + a^2B^2e^6. \tag{5.7}$$

Factorizing this equation yields the following expression:

$$m^3 = (n + ame - aBe^3)(n - ame + aBe^3).$$

It should be noted that $K[t]$ is a principal ideal domain, when K is any field. In particular $\mathbb{F}_q[t]$ is a principal ideal domain. Therefore we enjoy unique (up to units and ordering) factorization of elements and the notion of greatest common divisor is well-defined. Define

$$d := \gcd(n + ame - aBe^3, n - ame + aBe^3),$$

then we can write:

$$n - ame + aBe^3 = u_1dc_1 \text{ and } n + ame - aBe^3 = u_2dc_2,$$

for some coprime c_1, c_2 in $\mathbb{F}_q[t]$ and u_1, u_2 units. We factor c_1 into a part coprime to d (call it k) and another part which will be of the form $p_1^{r_1}\cdots p_w^{r_w}$, for some irreducible elements p_i that divide d and $r_i \in \mathbb{Z}$. Similarly, we decompose c_2 (in a part l and a part $q_1^{t_1}\cdots q_s^{t_s}$) and obtain:

$$\begin{aligned}m^3 &= (n + ame - aBe^3)(n - ame + aBe^3)\\ &= u_2dc_2u_1dc_1\\ &= u_1u_2kp_1^{r_1}\cdots p_w^{r_w}lq_1^{t_1}\cdots q_s^{t_s}d^2.\end{aligned}$$

Note that kl is coprime with $p_1^{r_1}\cdots p_w^{r_w}q_1^{t_1}\cdots q_s^{t_s}d^2$ and that k and l are both coprime as well, hence k must be a cube and we can write $n - ame + aBe^3 = u_1dp_1^{r_1}\cdots p_w^{r_w}f^3$, for some $f \in \mathbb{F}_q[t]$. This shows that

$$\begin{aligned}\alpha(\frac{m}{e^2}, \frac{n}{e^3}) &= \overline{\frac{n}{e^3} - a\frac{m}{e^2} + aB}\\ &= \overline{n - ame + aBe^3}\\ &= \overline{u_1dp_1^{r_1}\cdots p_w^{r_w}}.\end{aligned}$$

If we want to show that the image of α is finite we need to show the following lemma.

Lemma 5.7. *The irreducible factors of d are contained in a finite set.*

Proof. The greatest common divisor d can be rewritten as:

$$\begin{aligned} d &= \gcd(n + ame - aBe^3, n - ame + aBe^3) \\ &= \gcd(n + ame - aBe^3, n - ame + aBe^3 - (n + ame - aBe^3)) \\ &= \gcd(n + ame - aBe^3, -2ae(m - Be^2)) \\ &= \gcd(n + ae(m - Be^2), -2a(m - Be^2)), \end{aligned}$$

where in the last equality we used that $n + ae(m - Be^2)$ and e are coprime, because n and e are coprime.

Note that there are only a fixed, finite number of irreducible factors in $-2a$. Hence we will only look at the irreducible factors of $d' := \gcd(n + ae(m - Be^2), m - Be^2)$. If there are a finite number of them, then the lemma is proven.

Suppose that $n + ae(m - Be^2)$ and $m - Be^2$ have irreducible factors in common, then n and $m - Be^2$ have these same irreducible factors in common. Assume that we have

$$\begin{aligned} d' &= p_1 \cdots p_l, \\ n &= p_1 \cdots p_l s, \\ m - Be^2 &= p_1 \cdots p_l t, \end{aligned}$$

where the p_i are irreducible elements and $s, t \in \mathbb{F}_q[t]$ such that $\gcd(s, t) = 1$. Starting from equation (5.7) we get the following:

$$\begin{aligned} n^2 &= m^3 + a^2m^2e^2 - 2a^2Bme^4 + a^2B^2e^6 \\ n^2 &= m^3 + a^2m^2e^2 - a^2Bme^4 - a^2Be^4(m - Be^2) \\ p_1^2 \cdots p_l^2 s^2 &= m^3 + a^2m^2e^2 - a^2Bme^4 - a^2Be^4 p_1 \cdots p_l t \\ p_1^2 \cdots p_l^2 s^2 + a^2Be^4 p_1 \cdots p_l t &= m^3 + a^2m^2e^2 - a^2Bme^4 \\ p_1 \cdots p_l(p_1 \cdots p_l s^2 + a^2Be^4 t) &= m^3 + a^2me^2(m - Be^2) \\ p_1 \cdots p_l(p_1 \cdots p_l s^2 + a^2Be^4 t) &= m^3 + a^2me^2 p_1 \cdots p_l t \\ p_1 \cdots p_l(p_1 \cdots p_l s^2 + a^2Be^4 t - a^2me^2 t) &= m^3. \end{aligned}$$

This means that $p_1 \cdots p_l$ has to divide m as well and hence $p_1, \cdots, p_l$ are irreducible factors of both m and n. Looking at equation (5.7) again we see that

$$n^2 - m^3 - a^2m^2e^2 - 2a^2Bme^4 = a^2B^2e^6.$$

So any irreducible element that is both a factor of m and n must either be a factor of aB or e, but the latter is impossible as $\gcd(m, e) = \gcd(n, e) = 1$. We conclude that the irreducible factors of d' are from the set $\{p_i : p_i \text{ irreducible and } p_i | aB\}$ and therefore the irreducible factors of d are from the set $\{p_i : p_i \text{ irreducible and } p_i | 2aB\}$, which finishes the proof of Lemma 5.7. □

We can now conclude the proof of Theorem 5.6. Indeed, we have shown that the image of α is contained in the set

$$\{up_1^{\epsilon_1} \cdots p_j^{\epsilon_j} : \epsilon_i \in \{0, 1, 2\},\ u \in \mathbb{F}_q^*/\mathbb{F}_q^{*3} \text{ and } p_i | 2aB\},$$

where the p_i are monic irreducible elements. Now note that the number of elements in $\mathbb{F}_q^*/\mathbb{F}_q^{*3}$ is clearly finite. Therefore we can indeed conclude that α has finite image, as desired. □

Note that the image of α is finite for any field $K(t)$ for which it holds that K^*/K^{*3} is finite. In fact, if K is algebraically closed, then every unit is a cube. So K^*/K^{*3} is finite as well.

All that remains to be shown is that $\ker(\alpha) = \hat{\phi}(\bar{E}(L))$, which will take up the remaining part of this section. The upcoming results and proofs are adaptations from [3, Section 8.4.3 & 8.4.4].

Proposition 5.8. *The kernel of α is equal to the image of $\hat{\phi}$. Formally stated:*

$$\ker(\alpha) = \hat{\phi}(\bar{E}(L)).$$

Before we give the proof of this proposition, we first state and prove some useful lemmas about the image of the original mapping ϕ.

Lemma 5.9. *Recall that $\sqrt{-3} = \delta \in L$ and denote by $\hat{I} := \phi(E(L))$. The following two properties hold.*

(1) $\bar{\mathcal{O}} \in \hat{I}$ and $\pm\hat{T} = (0, \pm\delta a\bar{B}) \in \hat{I}$ if and only if $\frac{3a^2}{2\bar{B}}$ is a cube in L.

(2) A general point $\hat{P} = (\hat{x}, \hat{y}) \in \bar{E}(L)$ different from $\pm\hat{T}$ or $\bar{\mathcal{O}}$ belongs to $\hat{I}$ if and only if there exists $\gamma \in L$ such that $\gamma^3 = \hat{y} - (\hat{x} - \bar{B})\delta a$.

Proof. (1) By definition we have that $\hat{\phi}(\mathcal{O}) = \bar{\mathcal{O}}$ and hence $\bar{\mathcal{O}} \in \hat{I}$. Looking at the definition of ϕ we have that $\pm\hat{T} \in \hat{I}$ if and only if there exists $x \in L$ such that $x^3 + 4a^2(\frac{1}{3}x^2 - Bx + B^2) = 0$. Note that this implies that $x \neq 0$, because $B \neq 0$ as E is an elliptic curve. Plugging this into SageMath [10] (see Appendix A listing 2), we see that we have a rational solution if and only if $-64/729a^6 - 8/9Ba^4 + 2/27(4a^2 + 27B)Ba^2 - 2B^2a^2$ is a cube. Some algebra yields that this is equivalent to $-2a(9\bar{B})$ being a cube, which is equivalent to $\frac{(-18)^2a^2\bar{B}^2}{(6\bar{B})^3}$ being a cube. This is in turn equivalent to $\frac{3a^2}{2\bar{B}}$ being a cube, as desired.

(2) Note that $x = 0$ implies that $(x, y) = \pm T$, with $\pm T = (0, aB)$ and $\phi(\pm T) = \bar{\mathcal{O}}$. So we can assume that $x \neq 0$. Take $(x, y) \in \hat{I}$, some algebra yields:

$$\hat{y} - (\hat{x} - \bar{B})\delta a = \frac{\theta}{x^3},$$

where

$$\theta = y\left(x^3 + 4AB(x - 2B)\right) - \left(x^4 + 4Ax\left(\frac{1}{3}x^2 - Bx + B^2\right) - \frac{x^3}{9}(4A + 27B)\right)a\delta.$$

Letting SageMath simplify this (see Appendix A listing 1) and recalling that $A = a^2$ we obtain the following expression for θ:

$$\theta = -4B^2a^3\delta x + 4Ba^3\delta x^2 - a\delta x^4 - \frac{1}{9}\left(8a^3 - 27Ba\right)\delta x^3 - (8B^2a^2 - 4Ba^2x - x^3)y.$$

On the other hand we have that

$$\begin{aligned}\left(y - \left(\frac{1}{3}x - B\right)\delta a\right)^3 &= y^3 - 3y^2\left(\frac{1}{3}x - B\right)\delta a + 3y\left(\frac{1}{3}x - B\right)^2\delta^2a^2 - \left(\frac{1}{3}x - B\right)^3\delta^3a^3 \\ &= y^3 - 3y^2\left(\frac{1}{3}x - B\right)\delta a - 9y\left(\frac{1}{3}x - B\right)^2a^2 + 3\left(\frac{1}{3}x - B\right)^3\delta a^3.\end{aligned}$$

Plugging in $y^2 = x^3 + a^2(x-B)^2$ and letting SageMath simplify the expression we obtain:

$$\left(y - \left(\frac{1}{3}x - B\right)\delta a\right)^3 = \theta.$$

This shows that θ is a cube and hence $\hat{y} - (\hat{x} - \bar{B})\delta a$ is a cube as well, which finishes one implication.

Conversely, suppose that $(\hat{x}, \hat{y}) \in \bar{E}(L)$ such that there exists $\gamma \in L$ satisfying $\gamma^3 = \hat{y} - (\hat{x} - \bar{B})\delta a$. Note that $\gamma = 0$ yields $0 = \hat{y}^2 - (\hat{x} - \bar{B})^2\bar{A} = \hat{x}^3$ and hence $\hat{x} = 0$. But then we would have that our point is $\pm\hat{T}$, so in the present case $\gamma \neq 0$.

Lemma 5.10. *Set* $u = \frac{\gamma + \hat{x}/\gamma}{2}$ *and* $v = \frac{\gamma - \hat{x}/\gamma}{2a\delta}$. *We have*

(1) $(\hat{x}/\gamma)^3 = \hat{y} + (\hat{x} - \bar{B})a\delta$,

(2) $B = (v + 1/3)(u^2 - a^2(v - 2/3)^2)$.

Proof. (1) This should be clear as:

$$(\hat{x}/\gamma)^3 = \frac{\hat{y}^2 - \delta^2 a^2(\hat{x} - \bar{B})^2}{\hat{y} - \delta a(\hat{x} - \bar{B})} = \hat{y} + (\hat{x} - \bar{B})a\delta.$$

(2) We can write $\gamma = u + va\delta$ and $\hat{x}/\gamma = u - va\delta$, hence $\hat{x} = u^2 + 3a^2v^2$. We compute $\gamma^3 - (\hat{x}/\gamma)^3$ in two ways. On the one hand, we have

$$\gamma^3 - \frac{\hat{x}^3}{\gamma^3} = 6u^2va\delta + 2(va\delta)^3 = -2a\delta(3a^2v^3 - 3u^2v).$$

On the other hand we have

$$\gamma^3 - \frac{\hat{x}^3}{\gamma^3} = -2\delta a\left(u^2 + 3a^2v^2 - \frac{4a^2 + 27B}{9}\right).$$

Equating both these expressions and some elementary algebra proves the lemma. □

It is now relatively easy to finish the proof of Lemma 5.9. In fact, because $B \neq 0$ we have $v + \frac{1}{3} \neq 0$. Therefore we can define

$$x = \frac{B}{v + 1/3} = u^2 - a^2(v - 2/3)^2$$

and

$$y = ux = u^3 - ua^2(v - 2/3)^2.$$

We thus have $y^2 = u^2x^2 = \frac{u^2B^2}{(v+1/3)^2}$ and

$$\begin{aligned}(v + 1/3)^3(x^3 + a^2(x - B)^2) &= B^3 + (v + 1/3)^3a^2\left(\frac{B}{v + 1/3} - B\right)^2 \\ &= B^3 + a^2(v + 1/3)\left(B - (v + 1/3)B\right)^2 \\ &= B^3 + B^2a^2(v + 1/3)\left(2/3 - v\right)^2 \\ &= B^2(B + a^2(v + 1/3)(v - 2/3)^2) \\ &= B^2(v + 1/3)u^2.\end{aligned}$$

This in fact shows that $y^2 = x^3 + a^2(x-B)^2$ and hence $(x,y) \in E(L)$.

All that is left, is to show that $\phi(x,y) = (\hat{x}, \hat{y})$. Note that we have $\phi(x,y) = (\alpha, \beta)$ with

$$\begin{aligned}\alpha &= \frac{1}{x^2}(x^3 + 4a^2\left(\frac{1}{3}x^2 - Bx + B^2\right)\\ &= x + 4a^2\left(1/3 - B/x + (B/x)^2\right)\\ &= u^2 - a^2(v-2/3)^2 + a^2\left(4/3 - 4(v+1/3) + 4(v+1/3)^2\right)\\ &= u^2 + 3a^2v^2\\ &= \hat{x}.\end{aligned}$$

In a similar fashion is is found that $\beta = \hat{y}$, which finishes the proof of the lemma. □

The following is an immediate consequence by considering the dual isogeny.

Corollary 5.11. *Let $I := \hat{\phi}(\bar{E}(L))$. The following two properties hold.*

(1) $\mathcal{O} \in I$ and $\pm T = (0, \pm aB) \in I$ if and only if $\frac{-a^2}{2B}$ is a cube in L.

(2) A general point $P = (x,y) \in E(L)$ different from $\pm T$ or $\mathcal{O}$ belongs to I if and only if there exists $\gamma \in L$ such that $\gamma^3 = y - (x-B)a$.

We are now ready to give the proof of Proposition 5.8.

Proof of Proposition 5.8. The proof follows from the following three points.

(1) $\mathcal{O} \in \ker(\alpha)$ and clearly $\mathcal{O} \in \hat{\phi}(\bar{E}(L))$.

(2) $\pm T \in \ker(\alpha)$ if and only if $2aB$ is a cube in L, if and only if $\frac{4a^2B^2}{-8B^3}$ is a cube, if and only if $\frac{-a^2}{2B}$ is a cube, and hence by Corollary 5.11 if and only if $\pm T \in \hat{\phi}(\bar{E}(L))$.

(3) For any other point $(x,y) \notin \{\mathcal{O}, \pm T\}$ we have $(x,y) \in \ker(\alpha)$ if and only if $y - (x-B)a$ is a cube and by Corollary 5.11 if and only if $(x,y) \in \hat{\phi}(\bar{E}(L))$.

□

We are now almost ready to give a proof for Theorem 3.2. In fact, we have already proven it in the case when -3 is a perfect square and when $E\colon y^2 = x^3 + a^2(x-B)^2$. However, Theorem 3.2 does not require these assumptions and we need one more result before we can give a proof.

Lemma 5.12. *Let $q = p^n$ be a prime power with $p \notin \{2,3\}$, then we have that -3 is a perfect square in L if and only if $q \equiv 1 \bmod 6$.*

Proof. First note that -3 is a perfect square in L if and only if -3 is a perfect square in $\mathbb{F}_q$. Now if -3 is a perfect square in $\mathbb{F}_q$, then the existence of a cube root of unity in $\mathbb{F}_q$ is guaranteed. Therefore 3 divides $q-1$ and hence $q \equiv 1 \bmod 6$.

Conversely, let q be a prime power such that $q \equiv 1 \bmod 6$ and consider the finite field $\mathbb{F}_q$. Note that 3 divides $q-1$ and hence we have the existence of a primitive cube root of unity $\omega := \frac{-1+\sqrt{-3}}{2}$. Moreover, some rewriting yields that $\sqrt{-3} = 2\omega + 1$ and hence the square root of -3 is always in $\mathbb{F}_q$. □

It has been a long journey, but we are now finally able to present a proof for Theorem 3.2.

Proof of Theorem 3.2. The proof is done in four separate cases.

Case 1: Consider the elliptic curve $E\colon y^2 = x^3 + a^2(x-B)^2$, with $a, B \in \mathbb{F}_q[t]$. Moreover, suppose that -3 is a perfect square in L (which is equivalent to saying $q \equiv 1 \bmod 6$ by Lemma 5.12). Using Lemma 4.5, 4.6, 4.7 and the fact that $[E(L)\colon 3E(L)]$ is finite for the elliptic curve $E\colon y^2 = x^3 + a^2(x-B)^2$ we can conclude via the Descent theorem that $E(L)$ is finitely generated.

Case 2: Consider the same curve as in case 1, but now suppose that -3 is not a perfect square in L. From Lemma 5.12 we deduce that $q \not\equiv 1 \bmod 6$ and because the characteristic of $\mathbb{F}_q$ is not 2 or 3, we also have that $\gcd(q, 6) = 1$. Together this implies that $q \equiv -1 \bmod 6$, so $q^2 \equiv 1 \bmod 6$ and hence -3 is a perfect square in $\mathbb{F}_{q^2}$. Consider the elliptic curve $E\colon y^2 = x^3 + a^2(x-B)^2$ as before, but over $\mathbb{F}_{q^2}(t)$. So a and B are both in $\mathbb{F}_{q^2}[t]$ and the characteristic of our field is still not 2 or 3. Due to the fact that -3 is a square in $\mathbb{F}_{q^2}$, the previous paragraph tells us that $E(\mathbb{F}_{q^2}(t))$ is a finitely generated abelian group. Moreover, we know that $L \subset \mathbb{F}_{q^2}(t)$ and hence $E(L)$ is a subgroup of $E(\mathbb{F}_{q^2}(t))$. We can therefore conclude that $E(L)$ must be finitely generated as well.

Case 3: Consider the elliptic curve $E : y^2 = x^3 + c \cdot a^2(x-B)^2$, with $a, B \in \mathbb{F}_q[t]$ and $c \in \mathbb{F}_q$. If c is a perfect square, then the problem reduces to either case 1 or case 2. So in this case also $E(L)$ is finitely generated.

Case 4: Consider the curve from case 3, but suppose that c is not a perfect square. Consider the field extension $L(\sqrt{c}) \cong \mathbb{F}_{q^2}(t)$ and consider the curve $E\colon y^2 = x^3 + c \cdot a^2(x-B)^2$ over $L(\sqrt{c})$. Then $c \cdot a^2$ is a perfect square and we reduce to either case 1 or case 2. So also in this case, $E(L)$ is finitely generated.

The four cases above cover all possibilities and hence the theorem is proven. □

One might think that a similar type of reasoning works for general $c \in \mathbb{F}_q[t]$. However, if $c \in \mathbb{F}_q[t] \setminus \mathbb{F}_q$, then $L(\sqrt{c}) \ncong \mathbb{F}_{q^2}(t)$. So in this case we can not reduce to a simpler case as in the proof of Theorem 3.2. Next section we have a look at the computation of the rank, when it is possible. Moreover, we will look at some examples of this computation.

6 Computing the Rank

6.1 A Formula for the Rank

In the previous section it is shown that the group $E(\mathbb{F}_q(t))$ is finitely generated when $E : y^2 = x^3 + c \cdot a^2(x-B)^2$ with $a, B \in \mathbb{F}_q[t]$, $c \in \mathbb{F}_q$ and $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$. This section investigates the rank of the group $E(\mathbb{F}_q(t))$ whenever $q \equiv 1 \bmod 6$ and $c = 1$. If this is not the case the rank might be deduced by first determining the rank of E over some field extension M of $\mathbb{F}_q(t)$ and noting that $E(\mathbb{F}_q(t))$ must be a subgroup of $E(M)$, as we saw in the proof of Theorem 3.2. This section ends with some explicit examples of rank computations.

By the structure theorem of finitely generated abelian groups we have that

$$E(\mathbb{F}_q(t)) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}},$$

where $r \in \mathbb{Z}_{\geq 0}$ is the rank, the p_i are primes and the $\nu_i \in \mathbb{Z}_{>0}$.

For the sake of notation we again write $L := \mathbb{F}_q(t)$. From the above we have that every $P \in E(L)$ can be written as:

$$P = n_1P_1 + \cdots + n_rP_r + m_1Q_1 + \cdots + m_sQ_s.$$

Looking at $3E(L)$ we see that we can write

$$3E(L) \cong (3\mathbb{Z})^r \oplus 3\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus 3\mathbb{Z}_{p_s^{\nu_s}}$$

and hence the quotient is given as

$$E(L)/3E(L) \cong (\mathbb{Z}/3\mathbb{Z})^r \oplus \frac{\mathbb{Z}_{p_1^{\nu_1}}}{3\mathbb{Z}_{p_1^{\nu_1}}} \oplus \cdots \oplus \frac{\mathbb{Z}_{p_s^{\nu_s}}}{3\mathbb{Z}_{p_s^{\nu_s}}}.$$

This equation might look daunting, but the last s terms simplify quite nicely. In fact, we have

$$\frac{\mathbb{Z}_{p_i^{\nu_i}}}{3\mathbb{Z}_{p_i^{\nu_i}}} \cong \begin{cases} \mathbb{Z}/3\mathbb{Z}, & \text{if } p_i = 3 \\ \{0\}, & \text{if } p_i \neq 3. \end{cases}$$

Using this we can write $[E(L)\colon 3E(L)] = 3^{r+\text{number of } i \text{ such that } p_i = 3}$.

Denote $\Gamma := E(L)$ and write $\Gamma[3]$ for the subgroup of Γ consisting of points with order dividing 3, called the 3-torsion subgroup. We can relate the size of this subgroup to $[\Gamma\colon 3\Gamma]$ as follows. Let $P \in \Gamma[3]$ and write

$$3P = 3(n_1P_1 + \cdots n_rP_r + m_1Q_1 + \cdots m_sQ_s) = \mathcal{O}.$$

This tells us that $n_i = 0$ and $3m_j \equiv 0 \bmod p_j^{\nu_j}$. Now note that if $p_j \neq 3$, then $m_j = 0$ and if $p_j = 3$ we obtain that $m_j \equiv 0 \bmod p_j^{\nu_j - 1}$. Using this we see that $\#\Gamma[3] = 3^{\text{number of } j \text{ such that } p_j = 3}$ and hence we obtain the quite elegant formula for the rank:

$$3^r = \frac{[\Gamma\colon 3\Gamma]}{\#\Gamma[3]}.$$

We will rewrite this formula into more computable terms. Denote $\bar{\Gamma} := \bar{E}(L)$ and note that we have the subgroup inclusion: $3\Gamma \subseteq \hat{\phi}(\bar{\Gamma}) \subseteq \Gamma$. This gives that the index $[\Gamma\colon 3\Gamma]$ can be rewritten as

$$\begin{aligned}[\Gamma\colon 3\Gamma] &= [\Gamma\colon \hat{\phi}(\bar{\Gamma})][\hat{\phi}(\bar{\Gamma})\colon 3\Gamma] \\ &= [\Gamma\colon \hat{\phi}(\bar{\Gamma})][\hat{\phi}(\bar{\Gamma})\colon \hat{\phi} \circ \phi(\Gamma)].\end{aligned}$$

Before we continue we first state a lemma from group theory.

Lemma 6.1. *Let G be an abelian group and H a subgroup of finite index. Let $f : G \to G'$ be a homomorphism into some group G'. Then $[f(G)\colon f(H)] = \frac{[G\colon H]}{[\ker(f)\colon \ker(f) \cap H]}$.*

Proof. By the standard isomorphism theorems from group theory we have:

$$\begin{aligned}\frac{f(G)}{f(H)} &\cong \frac{G}{H + \ker(f)} \\ &\cong \frac{G/H}{(H + \ker(f))/H} \\ &\cong \frac{G/H}{\ker(f)/(H \cap \ker(f))},\end{aligned}$$

from which the desired result follows. □

Using Lemma 6.1 with $G = \bar{\Gamma}$ and $H = \phi(\Gamma)$ we find

$$3^r = \frac{[\Gamma\colon \hat{\phi}(\bar{\Gamma})][\bar{\Gamma}\colon \phi(\Gamma)]}{\#\Gamma[3] \cdot [\ker(\hat{\phi})\colon \ker(\hat{\phi}) \cap \phi(\Gamma)]}. \tag{6.1}$$

In Section 5 we have already established that $[\Gamma\colon \hat{\phi}(\bar{\Gamma})] = \#\alpha(\Gamma)$ and $[\bar{\Gamma}\colon \phi(\Gamma)] = \#\bar{\alpha}(\bar{\Gamma})$. So lets now focus on the denominator of the right-hand side of equation (6.1). The only elements that get mapped to $\mathcal{O}$ by $\hat{\phi}$ are $\bar{\mathcal{O}}$ and $(0, \pm\delta a\bar{B})$. From Lemma 5.9 we know that $(0, \delta a\bar{B}) \in \phi(\Gamma)$ if and only if $\frac{3a^2}{2\bar{B}}$ is a cube. This yields the following formula for the rank:

$$3^r = \begin{cases} \frac{\#\alpha(\Gamma)\cdot\#\bar{\alpha}(\bar{\Gamma})}{\#\Gamma[3]}, & \text{if } \frac{3a^2}{2\bar{B}} \text{ is a cube,} \\ \frac{\#\alpha(\Gamma)\cdot\#\bar{\alpha}(\bar{\Gamma})}{3\cdot\#\Gamma[3]}, & \text{otherwise.} \end{cases} \tag{6.2}$$

This formula tells us that once we know enough information about the images of α and $\bar{\alpha}$ and about the amount of 3-torsion, then we can calculate the rank explicitly. The next theorem, which is based on [4, Theorem 3.1], relates the image of α to the solvability of a cubic equation. This will come in handy when doing explicit examples.

Theorem 6.2. *Let $L := \mathbb{F}_q(t)$ and consider the elliptic curve $E\colon y^2 = x^3 + a^2(x-B)^2$, where $a, B \in \mathbb{F}_q[t]$. An element $\bar{u} \in L^*/L^{*3}$ not equal to $1, 2aB$ or $\frac{1}{2aB}$ modulo L^{*3} is in the image of α if and only if for every representative $u \in L^*$ of $\bar{u}$ the homogeneous cubic*

$$uX^3 + \frac{1}{u}Y^3 - 2aBZ^3 - 2aXYZ = 0$$

has an integral [†] (and hence rational) solution with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$.

Proof. "⇒" Let $\bar{u} \in L^*/L^{*3}$ be in the image of α. Recalling the definition of the map α we see that this is equivalent to saying that there exist $(x, y) \in E(L)$ such that $y - a(x-B) = uz^3$ for some $z \in L^*$. Set $X = z^2$, $Y = -x$ and $Z = z$, then we obtain:

$$\begin{aligned} uX^3 + \frac{1}{u}Y^3 - 2aBZ^3 - 2aXYZ &= \frac{1}{u}\left(u^2z^6 - x^3 - 2aBz^3u + 2axuz^3\right) \\ &= \frac{1}{u}\left(u^2z^6 - x^3 + 2uaz^3\,(x-B)\right) \\ &= \frac{1}{u}\left(\left(uz^3 + a\,(x-B)\right)^2 - x^3 - a^2\,(x-B)^2\right) \\ &= \frac{1}{u}(y^2 - y^2) \\ &= 0. \end{aligned}$$

This shows that the cubic equation is satisfied and because $z \in L^*$ we also have $Z \neq 0$. Moreover, because the equation is homogeneous we can multiply through by $\gcd(X, Y, Z)$ and hence assume that $\gcd(X, Y, Z) = 1$.

"⇐" Let (X, Y, Z) be a solution to the cubic with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. Set $x = \frac{-XY}{Z^2}$ and $y = \frac{uX^3 - (1/u)Y^3}{2Z^3}$, then we obtain:

$$\begin{aligned} x^3 + a^2(x-B)^2 &= \frac{-X^3Y^3}{Z^6} + a^2\left(\frac{-XY}{Z^2} - B\right)^2 \\ &= \frac{-X^3Y^3 + Z^2\left(-aXY - aBZ^2\right)^2}{Z^6}. \end{aligned}$$

[†] Meaning a solution with X, Y and Z in $\mathbb{F}_q[t]$.

From the cubic equation we obtain that $-aXY - aBZ^2 = \frac{-uX^3-(1/u)Y^3}{2Z}$ and hence:

$$\begin{aligned} x^3 + a^2(x-B)^2 &= \frac{-X^3Y^3 + (1/4)\left(uX^3 + (1/u)Y^3\right)^2}{Z^6} \\ &= \frac{-4X^3Y^3 + \left(uX^3 + (1/u)Y^3\right)^2}{4Z^6} \\ &= y^2, \end{aligned}$$

which shows that $(x, y) \in E(L)$. Moreover, we have that:

$$\begin{aligned} \alpha(x,y) &\equiv \frac{uX^3 - (1/u)Y^3}{2Z^3} + \frac{aXY + aBZ^2}{Z^2} \pmod{L^{*3}} \\ &\equiv \frac{1}{2Z^3}\left(uX^3 - (1/u)Y^3 + 2aXYZ + 2aBZ^3\right) \pmod{L^{*3}} \\ &\equiv \frac{1}{2Z^3} 2uX^3 \pmod{L^{*3}} \\ &\equiv u\left(\frac{X}{Z}\right)^3 \pmod{L^{*3}} \\ &\equiv u \pmod{L^{*3}}, \end{aligned}$$

which shows that (x, y) is indeed the preimage of u under α, as desired. □

With this machinery under our belt we are ready to tackle some examples. This is done in the remaining part of this thesis.

6.2 Explicit Examples

Before we continue with some examples we should note that finding $\#\Gamma[3]$ is rather easy for a given example, but not trivial to do in general. As discussed in Section 2.3, when considering elliptic curves over $\mathbb{Q}$ it is known that there are at most three $\mathbb{Q}$-rational points of order 3 on the curve. However, this does not hold for function fields of the form $\mathbb{F}_q(t)$. We will therefore not prove a general result regarding this, but we will deduce the amount of 3-torsion per example. Theorem 2.9, the rational root theorem, will be of big importance in doing so.

6.2.1 An Example of Rank 0

Consider the elliptic curve $E\colon y^2 = x^3 + (x-t)^2$ over $\mathbb{F}_7(t)$. In this case the points with x-coordinate zero are given by $\pm T = (0, \pm t)$ and the corresponding elliptic curve is given by $\bar{E}\colon y^2 = x^3 + 2^2(x - 2(3t+2))^2$, with $\pm\bar{T} = (0, \pm 2(3t+2))$. We have that $\frac{3}{4+6t}$ is not a cube in $\mathbb{F}_7(t)$ and hence we will be working with the formula

$$3^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{3 \cdot \#\Gamma[3]},$$

where $\Gamma := E(\mathbb{F}_7(t))$ and $\bar{\Gamma} := \bar{E}(\mathbb{F}_7(t))$. Lets first have a closer look at the 3-torsion of the elliptic curve. A point in $(x, y) \in E(\mathbb{F}_7(t))$ is of order 3 if and only if it is a root of $p_3(x) = 3x^4 + 4x^3 + 2t^2x^2 + 5t^2x$. The obvious rational root is given by $x = 0$ and in fact, this is the only rational root. To see this, suppose $\frac{p}{q}$ written in lowest terms would be a solution of $\frac{p_3(x)}{x} = 0$. By the rational root theorem we get that $q \mid 3$ and $p \mid 5t^2$. This yields that $q \in \{1, 3\}$

and $p \in \{1, 5, t, 5t, 5t^2\}$ and a quick check shows that none of these possibilities lead to $\frac{p_3(x)}{x} = 0$. Therefore, $x = 0$ is the only rational root of $p_3(x)$ and we conclude that $\#\Gamma[3] = 3$.

The mapping $\alpha\colon E(\mathbb{F}_7(t)) \to \mathbb{F}_7(t)^*/\mathbb{F}_7(t)^{*3}$ is given by

$$\begin{aligned} \mathcal{O} &\mapsto 1 \pmod{\mathbb{F}_7(t)^{*3}}, \\ T &\mapsto 2t \pmod{\mathbb{F}_7(t)^{*3}}, \\ -T &\mapsto \frac{1}{2t} \equiv 4t^2 \equiv 3t^2 \pmod{\mathbb{F}_7(t)^{*3}}, \\ (x, y) &\mapsto y - (x - t) \pmod{\mathbb{F}_7(t)^{*3}}, \end{aligned}$$

where we used that $1, 2$ and 3 are representatives for $\mathbb{F}_7^*/\mathbb{F}_7^{*3}$, so that $3 \equiv 4 \bmod \mathbb{F}_7(t)^{*3}$. Theorem 5.6 tells us that

$$\operatorname{im}(\alpha) \subset \{u p_1^{e_1} \cdots p_j^{e_j} : u \in \mathbb{F}_7^*/\mathbb{F}_7^{*3},\ p_i \mid 2t \text{ and } e_i \in \{0, 1, 2\}\},$$

where the p_i are monic irreducible elements. We conclude that an element z in the image of α must be of the form $z = ut^{e_1}$, with $e_1 \in \{0, 1, 2\}$ and $u \in \mathbb{F}_7^*/\mathbb{F}_7^{*3}$. As the number of elements in $\mathbb{F}_7^*/\mathbb{F}_7^{*3}$ is equal to $\frac{6}{2} = 3$ we get that $\#\alpha(\Gamma) \leq 9$ and hence $\#\alpha(\Gamma) \in \{3, 9\}$. Note that t is not the image of $\mathcal{O}$ or $\pm T$ under α. So whether $\#\alpha(\Gamma)$ is equal to 3 or 9 depends on whether t is in the image of α.

By Theorem 6.2 we have that $t \in \operatorname{im}(\alpha)$ if and only if the cubic

$$tX^3 + \frac{1}{t}Y^3 - 2tZ^3 - 2XYZ = 0$$

has an integral solution with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. In fact, we claim that such a solution does not exist. To see this first multiply the equation by t to obtain:

$$t^2X^3 + Y^3 - 2t^2Z^3 - 2tXYZ = 0. \tag{$\star$}$$

Suppose that ($\star$) has an integral solution (X, Y, Z) with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. Consider the polynomial $t + 3 \in \mathbb{F}_7[t]$, this polynomial is irreducible and hence the ideal $(t + 3)$ is maximal, thus prime. Moreover, we have that $\mathbb{F}_7[t]/(t + 3) \cong \mathbb{F}_7$ via $t \mapsto 4$. Reducing ($\star$) modulo this prime ideal yields the following cubic equation over $\mathbb{F}_7$:

$$2X^3 + Y^3 - 4Z^3 + 6XYZ = 0.$$

Checking all finite possibilities, we conclude that this equation has no nontrivial solution. Recalling that X, Y and Z are integral and such that $\gcd(X, Y, Z) = 1$ we can conclude that the original equation ($\star$) has no nontrivial solution and hence $\#\alpha(\Gamma) = 3$.

The mapping $\bar{\alpha}\colon \bar{E}(\mathbb{F}_7(t)) \to \mathbb{F}_7(t)^*/\mathbb{F}_7(t)^{*3}$ is given as

$$\begin{aligned} \bar{\mathcal{O}} &\mapsto 1 \pmod{\mathbb{F}_7(t)^{*3}}, \\ \bar{T} &\mapsto 4(2 + 3t) \equiv 5(t + 3) \equiv 2(t + 3) \pmod{\mathbb{F}_7(t)^{*3}}, \\ -\bar{T} &\mapsto \frac{1}{5(t + 3)} \equiv 4(t + 3)^2 \equiv 3(t + 3)^2 \pmod{\mathbb{F}_7(t)^{*3}}, \\ (\bar{x}, \bar{y}) &\mapsto \bar{y} - 2(\bar{x} - (2 + 3t)) \pmod{\mathbb{F}_7(t)^{*3}}. \end{aligned}$$

Similar reasoning as before shows that an element $z \in \mathrm{im}(\bar{\alpha})$ has to be of the form $z = u(t+3)^{e_1}$, with $u \in \mathbb{F}_7^*/\mathbb{F}_7^{*3}$ and $e_1 \in \{0,1,2\}$. So again, $\#\bar{\alpha}(\bar{\Gamma}) \in \{3,9\}$. Note that 2 is not the image of $\bar{\mathcal{O}}$ or $\pm\bar{T}$ under $\bar{\alpha}$. So consider the following cubic equation:

$$2X^3 + \frac{1}{2}Y^3 - 4(3t+2)Z^3 - 4XYZ = 0$$

and multiply by 2 to make it integral. This yields the cubic equation:

$$4X^3 + Y^3 + (4t+5)Z^3 - XYZ = 0. \tag{$\diamondsuit$}$$

We use the exact same reasoning as before, but now with the prime ideal (t). Reducing ($\diamondsuit$) modulo (t) yields the following cubic equation over $\mathbb{F}_7$:

$$4X^3 + Y^3 + 5Z^3 - XYZ = 0.$$

Checking all possibilities we find that this has no nontrivial solutions and hence we conclude that $\bar{\alpha}(\bar{\Gamma}) = 3$ and hence $3^{r+2} = 9$. We conclude that the rank of the elliptic curve is 0 and the computer algebra system Magma [1] agrees.

6.2.2 An Example of Rank 1

Consider the elliptic curve $E\colon y^2 = x^3 + 9^2(x-t^2)^2$ over $\mathbb{F}_{19}(t)$. In this case we have that the points with x-coordinate zero are given by $\pm T = (0, \pm 9t^2)$ and the corresponding elliptic curve is given by $\bar{E}\colon y^2 = x^3 + 2^2(x-(3t^2+17))^2$, with $\pm\bar{T} = (0, \pm 2(3t^2+17)) = (0, \pm 6(t+8)(t+11))$. We have that $\frac{3^5}{6t^2+15}$ is not a cube in $\mathbb{F}_{19}(t)$ and hence the formula for the rank is

$$3^r = \frac{\#\alpha(\Gamma)\cdot\#\bar{\alpha}(\bar{\Gamma})}{3\cdot\#\Gamma[3]},$$

where $\Gamma := E(\mathbb{F}_{19}(t))$ and $\bar{\Gamma} := \bar{E}(\mathbb{F}_{19}(t))$. In a similar fashion as in Section 6.2.1 we deduce that $\#\Gamma[3] = 3$.

The mapping $\alpha\colon E(\mathbb{F}_{19}(t)) \to \mathbb{F}_{19}(t)^*/\mathbb{F}_{19}(t)^{*3}$ is given by

$$\begin{aligned}
\mathcal{O} &\mapsto 1 \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
T &\mapsto 18t^2 \equiv t^2 \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
-T &\mapsto \frac{1}{t^2} \equiv t \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
(x,y) &\mapsto y - 9(x-t^2) \pmod{\mathbb{F}_{19}(t)^{*3}},
\end{aligned}$$

where we used that $1, 2$ and 4 are representatives for $\mathbb{F}_{19}^*/\mathbb{F}_{19}^{*3}$, so that $18 \equiv 1 \bmod \mathbb{F}_{19}(t)^{*3}$. Via Theorem 5.6 we obtain that an element z in the image of α must be of the form $z = ut^{e_1}$, with $e_1 \in \{0,1,2\}$ and $u \in \mathbb{F}_{19}^*/\mathbb{F}_{19}^{*3}$. There are 3 elements in $\mathbb{F}_{19}^*/\mathbb{F}_{19}^{*3}$ and hence we get that $\#\alpha(\Gamma) \leq 9$, so that $\#\alpha(\Gamma) \in \{3,9\}$. Note that 2 is not the image of $\mathcal{O}$ or $\pm T$ under α. So whether $\#\alpha(\Gamma)$ is equal to 3 or 9 depends on whether 2 is in the image of α.

By Theorem 6.2 we have that $2 \in \mathrm{im}(\alpha)$ if and only if the cubic

$$2X^3 + \frac{1}{2}Y^3 - 2\cdot 9t^2Z^3 - 2\cdot 9XYZ = 0$$

has an integral solution with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. We claim that such a solution can not exist. To see this first multiply the equation by 2 to obtain:

$$4X^3 + Y^3 + 2t^2Z^3 + 2XYZ = 0. \tag{♡}$$

Suppose that (♡) has an integral solution (X, Y, Z) with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. Consider the polynomial $t + 8 \in \mathbb{F}_{19}[t]$, this polynomial generates a prime ideal $(t + 8)$. Moreover, we have that $\mathbb{F}_{19}[t]/(t + 8) \cong \mathbb{F}_{19}$ via $t \mapsto -8$. Reducing (♡) modulo this prime ideal yields the following cubic equation over $\mathbb{F}_{19}$:

$$4X^3 + Y^3 + 14Z^3 + 2XYZ = 0.$$

This equation has no nontrivial solution over $\mathbb{F}_{19}$. Recalling that X, Y and Z are integral and such that $\gcd(X, Y, Z) = 1$ we can conclude that the original equation (♡) has no nontrivial solution and hence $\#\alpha(\Gamma) = 3$.

The mapping $\bar{\alpha}\colon \bar{E}(\mathbb{F}_{19}(t)) \to \mathbb{F}_{19}(t)^*/\mathbb{F}_{19}(t)^{*3}$ is given by

$$\begin{aligned}
\bar{\mathcal{O}} &\mapsto 1 \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
\bar{T} &\mapsto 4(3t^2 + 17) \equiv 12(t + 8)(t + 11) \equiv (t + 8)(t + 11) \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
-\bar{T} &\mapsto \frac{1}{(t + 8)(t + 11)} \equiv (t + 8)^2(t + 11)^2 \pmod{\mathbb{F}_{19}(t)^{*3}}, \\
(\bar{x}, \bar{y}) &\mapsto \bar{y} - 2(\bar{x} - (3t^2 + 17)) \pmod{\mathbb{F}_{19}(t)^{*3}}.
\end{aligned}$$

Similar reasoning as before shows that an element $z \in \mathrm{im}(\bar{\alpha})$ has to be of the form $z = u(t + 8)^{e_1}(t + 11)^{e_2}$, with $u \in \mathbb{F}_{19}^*/\mathbb{F}_{19}^{*3}$ and $e_1, e_2 \in \{0, 1, 2\}$. So we have, $\#\bar{\alpha}(\bar{\Gamma}) \in \{3, 9, 27\}$. A quick calculation shows that the point $(4t + 13, 6t^2 + 10t)$ lies on the curve $\bar{E}$ and

$$\begin{aligned}
\bar{\alpha}(4t + 13, 6t^2 + 10t) &\equiv 6t^2 + 10t - 2(4t + 13 - 3t^2 - 17) \pmod{\mathbb{F}_{19}(t)^{*3}} \\
&\equiv 12t^2 + 2t + 8 \pmod{\mathbb{F}_{19}(t)^{*3}} \\
&\equiv 12(t + 8)^2 \pmod{\mathbb{F}_{19}(t)^{*3}} \\
&\equiv (t + 8)^2 \pmod{\mathbb{F}_{19}(t)^{*3}}.
\end{aligned}$$

Note that $(t + 8)^2$ is not the image of $\bar{\mathcal{O}}$, $\bar{T}$ or $-\bar{T}$ under $\bar{\alpha}$ and hence $\#\bar{\alpha}(\bar{\Gamma}) \geq 9$. Using the fact that $\mathrm{im}(\bar{\alpha})$ is a group, it is not hard to see that

$$\mathcal{W} := \{1, t+8, (t+8)^2, (t+8)(t+11), (t+8)^2(t+11)^2, (t+8)^2(t+11), t+11, (t+11)^2, (t+8)(t+11)^2\}$$

must be contained in the image of $\bar{\alpha}$. Note that 2 is not among the elements of $\mathcal{W}$. So consider the following cubic equation:

$$2X^3 + \frac{1}{2}Y^3 - 4(3t^2 + 17)Z^3 - 4XYZ = 0$$

and multiply by 2 to make it integral. This yields the cubic equation:

$$4X^3 + Y^3 + 14(t + 8)(t + 11)Z^3 - 8XYZ = 0. \tag{♣}$$

Reducing (♣) modulo the prime ideal (t) yields the following cubic equation over $\mathbb{F}_{19}$:

$$4X^3 + Y^3 + 16Z^3 - 8XYZ = 0.$$

This equation has no nontrivial solutions and hence we conclude that $\bar{\alpha}(\bar{\Gamma}) = 9$. Therefore we must have $3^{r+2} = 27$, so that the rank of the elliptic curve is 1. The computer algebra system Magma agrees.

6.3 Choice of Prime Ideals and Solvability of the Cubic

In the previous examples we miraculously came up with a prime ideal $\mathfrak{p}$ and brute forced our way through solving a cubic equation in $\mathbb{F}_q[t]/\mathfrak{p}$. This section aims to explain in more depth the choice of prime ideals and tries to come up with a more elegant method of determining solvability of the cubic in $\mathbb{F}_q[t]/\mathfrak{p}$. The problem, which is closely related to [4, Section 5], is about solvability of cubic equations of the form

$$u_1X^3 + u_2Y^3 + u_3Z^3 - cXYZ = 0, \tag{6.3}$$

where u_1, u_2, u_3 and c are in $\mathbb{F}_q[t]$. One should note that when we talk about a solution to a homogeneous cubic equation over $\mathbb{F}_q[t]$, we always mean a nontrivial solution (X, Y, Z) with $\gcd(X, Y, Z) = 1$. The next lemma, adapted from [4, Lemma 5.3], for which we sketch the proof, gives us something to hold on to when searching for prime ideals.

Lemma 6.3. *Consider the cubic equation given by (6.3) and recall that* $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$. *Let* $\mathfrak{p}$ *be a prime ideal not dividing* $d := u_1u_2u_3(27u_1u_2u_3 - c^3)$, *then the cubic has a nontrivial solution over* $\mathbb{F}_q[t]/\mathfrak{p}^n$ *for all* $n \in \mathbb{Z}_{\geq 1}$.

Proof. Let $\mathfrak{p}$ be a prime ideal not dividing d and note that the cubic equation given by (6.3) defines a plane projective curve. We claim that reducing the coefficients modulo $\mathfrak{p}$ yields a nonsingular plane projective curve over $\mathbb{F}_q[t]/\mathfrak{p}$. First, a point with $Z = 0$ is singular (See Definition 2.7) if and only if $u_1X^3 + u_2Y^3 = 0$, $3u_1X^2 = 0$ and $3u_2Y^2 = 0$. As $\mathfrak{p} \nmid d$ and $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$ we have $X = Y = 0$, which is not possible. Thus any singular point has $Z \neq 0$, so we may assume that $Z = 1$. In this case we have a singular point if and only if $3u_1X^2 - cY = 0$, $3u_2Y^2 - cX = 0$ and $3u_3 - cXY = 0$. If there is such a singular point we can not have $c = 0$, otherwise $u_3 = 0$, but $\mathfrak{p} \nmid d$. Thus $Y = \frac{3u_1X^2}{c}$, $X = \frac{3u_2Y^2}{c} = \frac{27u_1^2u_2X^4}{c^3}$, hence either $X = 0$, which impossible since otherwise $X = Y = 0$ hence $u_3 = 0$, or $X^3 = \frac{c^3}{27u_1^2u_2}$, so that $3u_3 = cXY = 3u_1X^3 = \frac{c^3}{9u_1u_2}$. In other words $27u_1u_2u_3 - c^3 = 0$, which is also excluded as $\mathfrak{p} \nmid d$. Hence the cubic is nonsingular over $\mathbb{F}_q[t]/\mathfrak{p}$.

Using the Hasse-Weil bound[†] [9, Theorem 4.1] we obtain that our reduced cubic curve always has a rational point. Hensel's lemma [8, Section IV; Lemma 1.2] then shows that this solution lifts to a solution in $\mathbb{F}_q[t]/\mathfrak{p}^n$ for all $n \in \mathbb{Z}_{\geq 1}$, as desired. □

So in order to show that a cubic equation of the form given by equation (6.3) has no solution we only have to look for prime ideals occurring in the factorization of $d = u_1u_2u_3(27u_1u_2u_3 - c^3)$. To illustrate this, recall the example from Section 6.2.2. In this case we wanted to show that the cubic equation

$$4X^3 + Y^3 + 2t^2Z^3 + 2XYZ = 0$$

over $\mathbb{F}_{19}[t]$ has no rational solution with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. Looking at $d = 8t^2\left(27 \cdot 8t^2 - (-2)^3\right) = 18t^2(t + 8)(t + 11)$ we see that the prime ideal that worked ($\mathfrak{p} = (t + 8)$) indeed shows up in the factorization of d.

After factorizing d and having a candidate prime ideal $\mathfrak{p}$ we reduced the cubic equation modulo $\mathfrak{p}$ and checked all triples (X, Y, Z) in the residue field $\mathbb{F}_q[t]/\mathfrak{p}$. However, this brute force method can quite quickly get of hand as q gets bigger. The question arises is whether we can

[†]The Hasse-Weil bound gives a lower and upper bound for the number of rational points on algebraic curves over finite fields.

reduce our search for solutions. In fact, the answer to this question is in the affirmative. To see this, consider the cubic equation over $\mathbb{F}_q$ of the form:

$$aX^3 + bY^3 + cZ^3 - dXYZ = 0, \tag{6.4}$$

where $a, b, c, d \in \mathbb{F}_q$. The following lemma reduces the search for solutions tremendously.

Lemma 6.4. *Consider the equation given by (6.4). We have that (x, y, z) is a solution with $z \neq 0$ if and only if $(x/z, y/z, 1)$ is a solution.*

Proof. For any homogeneous equation in 3 variables we have that (x, y, z) is a solution if and only if (cx, cy, cz) is a solution for all $c \neq 0$. □

Using Lemma 6.4 we can set $Z = 1$ in equation (6.4). So we end up looking for solutions to

$$ax^3 + by^3 + c - dxy = 0,$$

which reduces the search to q^2 elements, a drastic decrease in computation time.

The study of equations of the form given by equation (6.3) can become quite elaborated. It is therefore that we finish our study towards these type of equations. We should acknowledge that this section did not give a proper method of deciding solvability or not, but at least it gave us some tools on how to approach them. In fact, there is no general algorithm that determines the solvability of the cubics we considered. There are only methods to show:

(1) that there is a solution, which means trying to find it;

(2) that there is no solution by reducing modulo powers of prime ideals.

However, some equations do not have integral (and hence rational) solutions even though they have solutions modulo every power of a prime ideal. To conclude the study of solvability of our cubic we should note that we either; try to find a solution, try to prove no solution exists or give up. In the latter case we can only give bounds on the rank of an elliptic curve.

7 A Different Elliptic Curve

7.1 Defining the Mappings

Recall that in Section 5.1 we showed that we have an elliptic curve of a particular form. However, the observant reader might have noticed that at some point we imposed the condition $b \neq 0$. In fact, assuming that $b = 0$ yields a completely different curve. Namely the elliptic curve given by:

$$E : y^2 = x^3 + c^2, \tag{7.1}$$

where c is some polynomial in $\mathbb{F}_q[t]$. This section is dedicated to proving that also $E(\mathbb{F}_q(t))$ is finitely generated, where E is the elliptic curve given by (7.1).

It is important to notice that we have already proven the first three properties of the Descent theorem (Theorem 3.3) for any elliptic curve E over $\mathbb{F}_q(t)$ with $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$, so we only have to show finiteness of the index. Due to the extreme similarities with Section 5 and [3, Section 8.4] we will only state, but not prove the upcoming statements. With this having said we take a q such that -3 is a square, write $\delta := \sqrt{-3} \in \mathbb{F}_q(t)$ and $L := \mathbb{F}_q(t)$, as before. In this case we

define the curve $\bar{E}\colon y^2 = x^3 + \bar{c}^2$, with $\bar{c} := 3\delta c$. It is not hard to see that the curve $\bar{\bar{E}}$ is given as $\bar{\bar{E}}\colon y^2 = x^3 + 3^6c^2$, which is isomorphic (See Definition 2.13) to E by replacing x with $9x$ and y with $27y$. The points with x-coordinate 0 are points of order 3 and on E they are given as $\pm T = (0, \pm c)$. On $\bar{E}$ the points with x-coordinate 0 are given as $\pm\bar{T} = (0, \pm 3\delta c)$. We now state some results regarding these curves.

Theorem 7.1. *Define the isogeny $\phi\colon E(\overline{L}) \to \bar{E}(\overline{L})$ as*

$$\begin{aligned} \pm T &\mapsto \bar{\mathcal{O}}, \\ \mathcal{O} &\mapsto \bar{\mathcal{O}}, \\ (x, y) &\mapsto \left(\frac{1}{x^2}\left(x^3 + 4c^2\right), \frac{y}{x^3}\left(x^3 - 8c^2\right) \right) \end{aligned}$$

and the isogeny $\hat{\phi}\colon \bar{E}(\overline{L}) \to E(\overline{L})$ as

$$\begin{aligned} \pm\bar{T} &\mapsto \mathcal{O}, \\ \bar{\mathcal{O}} &\mapsto \mathcal{O}, \\ (\bar{x}, \bar{y}) &\mapsto \left(\frac{1}{9\bar{x}^2}\left(\bar{x}^3 - 108c^2\right), \frac{\bar{y}}{27\bar{x}^3}\left(\bar{x}^3 - 216c^2\right) \right), \end{aligned}$$

where $\overline{L}$ is some fixed algebraic closure of L. Then we have $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [3]$, where $[3]$ stands for multiplication by 3 on the elliptic curve.

Lemma 7.2. *Let $\hat{I} := \phi(E(L))$. We have the following two statement about $\hat{I}$:*

(1) $\bar{\mathcal{O}} \in \hat{I}$ and $\pm\bar{T} \in \hat{I}$ if and only if $\frac{-1}{2c}$ is a cube.

(2) A general point $(\bar{x}, \bar{y}) \in \bar{E}(L)$ not equal to $\pm\bar{T}$ or $\bar{\mathcal{O}}$ is in $\hat{I}$ if and only if there exists $\gamma \in L$ such that $\gamma^3 = \bar{y} - 3\delta c$.

Similar results also hold for the image of the mapping $\hat{\phi}$.

Theorem 7.3. *Define the mapping $\alpha\colon E(L) \to L^*/L^{*3}$ as*

$$\begin{aligned} \mathcal{O} &\mapsto 1 \pmod{L^{*3}}, \\ T &\mapsto 2c \pmod{L^{*3}}, \\ -T &\mapsto \frac{1}{2c} \pmod{L^{*3}}, \\ (x, y) &\mapsto y - c \pmod{L^{*3}}. \end{aligned}$$

The following properties regarding α are true.

(1) The mapping α is a group homomorphism.

(2) $\mathrm{Im}(\alpha) \subset \{u p_1^{e_1} \cdots p_j^{e_j} : u \in \mathbb{F}_q^*/\mathbb{F}_q^{*3},\ p_i \mid 2c$ and $e_i \in \{0, 1, 2\}\}$.

(3) $\mathrm{Ker}(\alpha) = \hat{\phi}(\bar{E}(L))$.

Similar results also hold for the mapping $\bar{\alpha}\colon \bar{E}(L) \to L^*/L^{*3}$.

The proofs of these results follow a similar reasoning as the results from Section 5. Using these results and following a similar path as done in Section 5 we indeed obtain that $E(L)$ is finitely generated, when -3 is perfect square in L. However, as seen in the proof of 3.2 this assumption can be dropped by looking at $E(\mathbb{F}_{q^2}(t))$. Moreover, following the proof of Theorem 3.2 we can also deduce that $E(\mathbb{F}_q(t))$ is finitely generated, when $E\colon y^2 = x^3 + d \cdot c^2$ with $c \in \mathbb{F}_q[t]$ and $d \in \mathbb{F}_q$. Assuming that -3 is a perfect square in L and that $d = 1$, defining $\Gamma := E(L)$ and $\bar{\Gamma} := \bar{E}(L)$, and recalling Section 6.1 yields the following formula for the rank:

$$3^r = \begin{cases} \frac{\#\alpha(\Gamma)\cdot\#\bar{\alpha}(\bar{\Gamma})}{\#\Gamma[3]}, & \text{if } \frac{-1}{2c} \text{ is a cube,} \\ \frac{\#\alpha(\Gamma)\cdot\#\bar{\alpha}(\bar{\Gamma})}{3\cdot\#\Gamma[3]}, & \text{otherwise.} \end{cases} \tag{7.2}$$

7.2 Example of Higher Rank

In this section we will assume that $d = 1$ and that $q \equiv 1 \bmod 6$, so that by Lemma 5.12 we then have that -3 is a perfect square. As turns out, this choice of q also implies that the elliptic curve given by equation (7.1) admits an automorphism of order 3 defined over $\mathbb{F}_q(t)$. The next definition precisely states what an automorphism of elliptic curves means.

Definition 7.4. *Let E be an elliptic curve defined over a field K. An automorphism ρ of E is an isomorphism (See Definition 2.13) from E to itself.*

Example 7.5. *Let q be a prime power such that $q \equiv 1 \bmod 6$ and let $E\colon y^2 = x^3 + c^2$ be an elliptic curve with $c \in \mathbb{F}_q[t]$. Moreover, let $\rho\colon E(\overline{\mathbb{F}_q(t)}) \to E(\overline{\mathbb{F}_q(t)})$ be the mapping given by $\rho(x, y) := (\omega x, y)$, where ω is a cube root of unity and $\overline{\mathbb{F}_q(t)}$ a fixed algebraic closure of $\mathbb{F}_q(t)$. Then we have that ρ is an automorphism of order 3 defined over $\mathbb{F}_q(t)$.*

Recall that ρ restricts to a group homomorphism from $E(\mathbb{F}_q(t))$ to itself and that the notation $[1]$ stands for multiplication by one on an elliptic curve. In our case we have $\rho^3 = [1]$ and hence $(\rho - [1])(\rho^2 + \rho + [1]) = 0$. It is clear that $\rho \neq [1]$ and therefore $\rho^2 = -\rho - [1]$. Consider the set $\mathbb{Z}[\rho]$ given by

$$\mathbb{Z}[\rho] = \{a + b\rho\colon a, b \in \mathbb{Z}\} \subset \mathrm{End}(E),$$

where $\mathrm{End}(E)$ is the set of all isogenies from E to E. This inclusion follows from the fact that

$$\begin{aligned} g\colon \mathbb{Z} &\to \mathrm{End}(E), \\ n &\mapsto [n] \end{aligned}$$

is an injective ring homomorphism. The following lemma will be useful for determining the rank of $E(\mathbb{F}_q(t))$.

Lemma 7.6. *The set $\mathbb{Z}[\rho] = \{a + b\rho\colon a, b \in \mathbb{Z}\}$ is a principal ideal domain.*

Proof. Let $\omega \in \mathbb{C}$ be such that $\omega^2 + \omega + 1 = 0$. Consider the mapping

$$\begin{aligned} f\colon \mathbb{Z}[\omega] &\to \mathbb{Z}[\rho], \\ a + b\omega &\mapsto a + b\rho. \end{aligned}$$

The mapping f defines a ring isomorphism, and because $\mathbb{Z}[\omega]$ is a Euclidean ring we obtain that $\mathbb{Z}[\rho]$ is Euclidean ring and hence a principal ideal domain. □

The set $\mathbb{Z}[\rho]$ acts on $E(\mathbb{F}_q(t))$ via:

$$\begin{aligned} \mathbb{Z}[\rho] \times E(\mathbb{F}_q(t)) &\to E(\mathbb{F}_q(t)), \\ (a+b\rho,(x,y)) &\mapsto a(x,y)+b\rho(x,y), \end{aligned} \tag{7.3}$$

where '+' denotes addition on the elliptic curve and $a(x,y)$ usual scalar multiplication by a on the elliptic curve. This makes the Mordell-Weil group $E(\mathbb{F}_q(t))$ a module over $\mathbb{Z}[\rho]$ and the structure theorem for modules over principal ideal domains tells us that

$$E(\mathbb{F}_q(t)) \cong (\mathbb{Z}[\rho])^r \oplus T$$

as $\mathbb{Z}[\rho]$-modules, where T is the torsion part of $E(\mathbb{F}_q(t))$.

Note that when looking at the rank of $E(\mathbb{F}_q(t))$ we do so considering this set as a finitely generated abelian group and not as a $\mathbb{Z}[\rho]$-module. However, we know that abelian groups are just $\mathbb{Z}$-modules and as a $\mathbb{Z}$-module $\mathbb{Z}[\rho]$ has rank 2. So the Mordell-Weil rank[†] of $E(\mathbb{F}_q(t))$ must be an even integer.

In order do compute the rank explicitly we need to know when elements are in the image of α or $\bar{\alpha}$. The following theorem is analogous to Theorem 6.2, but for elliptic curves of the form $E\colon y^2 = x^3 + c^2$.

Theorem 7.7. *Let $L := \mathbb{F}_q(t)$ and consider the elliptic curve $E\colon y^2 = x^3 + c^2$, where $c \in \mathbb{F}_q[t]$. An element $\bar{u} \in L^*/L^{*3}$ not equal to $1, 2c$ or $\frac{1}{2c}$ modulo L^{*3} is in the image of α if and only if for every representative $u \in L^*$ of $\bar{u}$ the homogeneous cubic*

$$uX^3 + \frac{1}{u}Y^3 + 2cZ^3 = 0$$

has an integral (and hence rational) solution with $Z \neq 0$ and $\gcd(X,Y,Z) = 1$.

Proof. (Recall the proof of Theorem 6.2) "⇒" Let $\bar{u} \in L^*/L^{*3}$ be in the image of α. Recalling the definition of the map α we see that this is equivalent to saying that there exist $(x,y) \in E(L)$ such that $y - c = uz^3$ for some $z \in L^*$. Setting $X = z^2$, $Y = -x$ and $Z = z$ yields the desired result.

"⇐" Let (X,Y,Z) be a solution to the cubic with $Z \neq 0$ and $\gcd(X,Y,Z) = 1$. Setting $x = \frac{-XY}{Z^2}$ and $y = \frac{uX^3 - (1/u)Y^3}{2Z^3}$ yields the desired result. □

Now that we have all of the necessary information we can consider a specific example. Consider the elliptic curve $E\colon y^2 = x^3 + (t(t+3))^2$ over $\mathbb{F}_{13}(t)$. We have that $\sqrt{-3} = 6$ and the corresponding elliptic curve is $\bar{E}\colon y^2 = x^3 + (5t(t+3))^2$. To ease up some notation, write $\Gamma := E(\mathbb{F}_{13}(t))$ and $\bar{\Gamma} := \bar{E}(\mathbb{F}_{13}(t))$.

A point $P \neq \mathcal{O}$ is a point of order 3 if and only if the x-coordinate of P is a solution to

$$3x^4 + 12t^2(t+3)^2x = 0.$$

A quick check using the rational root theorem shows that only $x = 0$ is a rational solution and we deduce that $\#\Gamma[3] = 3$. Moreover, we have that $\frac{-1}{2t(t+3)}$ is not a cube in $\mathbb{F}_{13}(t)$ and hence we have the following formula for the rank:

$$3^{r+2} = \#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma}).$$

[†]Meaning the rank as a finitely generated abelian group.

$1, 2$ and 4 are representatives for $\mathbb{F}_{13}^*/\mathbb{F}_{13}^{*3}$ and the mapping $\alpha\colon E(\mathbb{F}_{13}(t)) \to \mathbb{F}_{13}(t)^*/\mathbb{F}_{13}(t)^{*3}$ is given by

$$\begin{aligned}
\mathcal{O} &\mapsto 1 \pmod{\mathbb{F}_{13}(t)^{*3}}, \\
T &\mapsto 2t(t+3) \pmod{\mathbb{F}_{13}(t)^{*3}}, \\
-T &\mapsto 4t^2(t+3)^2 \pmod{\mathbb{F}_{13}(t)^{*3}}, \\
(x,y) &\mapsto y - t(t+3) \pmod{\mathbb{F}_{13}(t)^{*3}},
\end{aligned}$$

where $\pm T = (0, \pm c) = (0, \pm t(t+3))$. It is not hard to check that $(t, t^2+10t) \in E(\mathbb{F}_{13}(t))$ and that $\alpha(t, t^2+10t) = 4t$. We can conclude that $\#\alpha(\Gamma) \geq 9$ and from Theorem 7.3 we obtain that an element z in the image of α has to be of the form $z = ut^{e_1}(t+3)^{e_2}$. So an upper bound for the size of the image of α is 27. Moreover, using the fact that $\mathrm{im}(\alpha)$ is a group we quite easily find that the set

$$\{1, 2(t+3), 4t^2(t+3)^2, 4t^2, 2t^2, t^2(t+3), t(t+3)^2, 2(t+3)^2, 4(t+3)\}$$

has to be contained in the image of α. Now note that $2 \in \mathbb{F}_{13}^*/\mathbb{F}_{13}^{*3}$ is not among these elements and is in the image of α if and only if

$$2X^3 + (1/2)Y^3 + 2t(t+3)Z^3 = 0$$

has an integral solution with $Z \neq 0$ and $\gcd(X, Y, Z) = 1$. So multiply this equation by 2, which gives us

$$4X^3 + Y^3 + 4t(t+3)Z^3 = 0$$

Reducing this equation modulo the prime ideal (t) yields

$$4X^3 + Y^3 = 0$$

over $\mathbb{F}_{13}$, which has no nontrivial solution. Hence t has to divide both X and Y, and because

$$Z^3 = \frac{-4X^3 - Y^3}{4t(t+3)}$$

we also get that t divides Z. However, then $\gcd(X, Y, Z)$ would not be 1, from which we conclude that our initial equation has no nontrivial solution. We can conclude that $\#\alpha(\Gamma) = 9$ and in a similar fashion it is found that $\#\bar{\alpha}(\bar{\Gamma}) \in \{9, 27\}$. Combining these results we obtain that the rank of $E(\mathbb{F}_{13}(t))$ is 2 or 3, but because the rank has to be even we obtain that the rank is 2.

8 Discussion & Further Developments

Computing the rank of an elliptic curve is not an easy task. We have explored the realm of elliptic curves over $\mathbb{F}_q(t)$ with $\mathrm{char}(\mathbb{F}_q) \notin \{2, 3\}$, which admit a rational point of order 3. This allowed us to rewrite the elliptic curve to the form

$$E\colon y^2 = x^3 + A(x-B)^2, \tag{8.1}$$

where $A = a^2$ and B are both in $\mathbb{F}_q[t]$. Or to the form

$$E\colon y^2 = x^3 + c^2, \tag{8.2}$$

with $c \in \mathbb{F}_q[t]$. In both cases we have shown that $E(\mathbb{F}_q(t))$ is a finitely generated abelian group. In fact, we managed to proof that the groups of $\mathbb{F}_q(t)$-rational point on more general curves are also finitely generated. These curves are of the form $E_1 \colon y^2 = x^3 + e \cdot a^2(x-B)^2$ and $E_2 \colon y^2 = x^3 + d \cdot c^2$, with $e, d \in \mathbb{F}_q$ and $a, B, c \in \mathbb{F}_q[t]$. These results have been proved using an explicit descent by 3-isogeny and it gave us an explicit way of computing the rank of the group $E(\mathbb{F}_q(t))$, when E is of the form given by equation (8.1) or (8.2). In order to compute the rank of these groups we needed a criteria on the (un)solvability of a homogeneous cubic over $\mathbb{F}_q(t)$. No general statement regarding the solvability of this cubic is known and in the examples we discussed we got quite lucky in proving unsolvability. However, some useful tools in determining this solvability have been given.

The main issue that we avoided by admitting a point of order 3 is the subject of algebraic number theory over function fields. In fact, when we loosen the assumption that $A \in \mathbb{F}_q(t) \setminus \mathbb{F}_q$ is a perfect square in (8.1), we need to work over a field extension of the form $\mathbb{F}_q(t)(\sqrt{A}) \ncong \mathbb{F}_{q^2}(t)$. This gets more complicated, because we do not necessarily enjoy unique factorization as we had with $\mathbb{F}_q[t]$.

Suggestions for further research include: finding similar statements as discussed in [4, Section 5], but over function fields of the form $\mathbb{F}_q(t)$ or proving that $E(\mathbb{F}_q(t))$ is finitely generated for an elliptic curve E, which does not necessarily admit a rational point of order 3 so that we have to work over a field extension without having unique factorization.

A Code Snippets

```
sage: x,y,delta,a,B = var('x y delta a B');
sage: z = y*(x^3+a^2*(x-B)^2) - 3*(x^3+a^2*(x-B)^2)*((1/3)*x-B)*delta*a -
    9*y*((1/3)*x - B)^2*a^2 + 3*((1/3)*x-B)^3*delta*a^3;
sage: z.full_simplify();
sage: k = y*(x^3 + 4*a^2*B*(x-2*B)) - (x^4 + 4*a^2*x*((1/3)*x^2 - B*x + B
    ^2)-x^3*((4*a^2+27*B)/9))*a*delta;
sage: k.full_simplify();
```

Listing 1: Code used in Lemma 5.9

```
sage: x,a,B,delta = var('x a B delta');
sage: LHS = x^3 + 4*a^2*((1/3)*x^2 -B*x+B^2);
sage: equation = (LHS == 0);
sage: solve(equation,x)
```

Listing 2: Code used in Lemma 5.9

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[2] W.H. Bussey. Fermat's Method of Infinite Descent. *The American Mathematical Monthly*, 25(8):333–337, 1918.

[3] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*, volume 239. Springer Science & Business Media, 2008.

[4] Henri Cohen and Fabien Pazuki. Elementary 3-Descent With a 3-Isogeny. *Acta Arithmetica*, 140(4):396–404, 2009.

[5] Gove Effinger, Kenneth Hicks, and Gary L. Mullen. Integers and Polynomials: Comparing the Close Cousins $\mathbb{Z}$ and $\mathbb{F}_q[x]$. *The Mathematical Intelligencer*, 27(2):26–34, 2005.

[6] Serge Lang and André Néron. Rational Points of Abelian Varieties over Function Fields. *American Journal of Mathematics*, 81(1):95–118, 1959.

[7] Louis Mordell. On the Rational Solutions of the Indeterminate Equation of the Third and Fourth Degree. In *Proc. Camb. Phil. Soc.*, volume 21, pages 179–192, 1992.

[8] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Science & Business Media, 2nd edition, 2009.

[9] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, 2nd edition, 2015.

[10] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. https://www.sagemath.org.

[11] Jaap Top. Rijksuniversiteit Groningen, Lecture Notes: Algebraic Structures, April 2017.

[12] Douglas Ulmer. Elliptic Curves and Analogies Between Number Fields and Function Fields. Heegner Points and Rankin L-series, 285–315. *Math. Sci. Res. Inst. Publ*, 49, 2004.

[13] Monique van Beek. Elliptic Curves of a Particular Form. Master's thesis, Rijksuniversiteit Groningen, 2010.

[14] José F. Voloch. Explicit p-descent for Elliptic Curves in Characteristic p. *Compositio Mathematica*, 74(3):247–258, 1990.

[15] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC press, 2008.

[16] Andrew Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.

[17] Andrew Wiles. The Birch and Swinnerton-Dyer Conjecture, 2006.

[18] Anne Wouda. Mordell's Theorem for Elliptic Curves over Rational Function Fields. Bachelor's thesis, Rijksuniversiteit Groningen, 2019.